Biblioteka Matematyczna

tom 59

BM

Witold Lipski, Wiktor Marek

Analiza kombinatoryczna

Państwowe Wydawnictwo Naukowe

BIBLIOTEKA MATEMATYCZNA

TOM 59

PAŃSTWOWE WYDAWNICTWO NAUKOWE

Mohyliv-Podilskyi 2022

WITOLD LIPSKI, WIKTOR MAREK

Analiza kombinatoryczna

przy współpracy *Michała Jaegermanna*

WARSZAWA 1986

Tytuł dotowany przez Ministra Nauki i Szkolnictwa Wyższego

Obwolutę i okładkę projektował
Roman Duszek

Redaktor techniczny
Eugeniusz Szkudaj

Korekta
Zespół

ISBN 83-01-04972-3
ISSN 0519-8356

PRZEDMOWA

Książka ta powstała jako wyraz długoletnich zainteresowań obu autorów kombinatoryką i jej zastosowaniami. Prowadziliśmy wykłady z tej dziedziny na Uniwersytecie Warszawskim oraz w Instytucie Podstaw Informatyki PAN. Brak podręcznika, który pokrywałby nowocześnie pojęty wykład kombinatoryki, skłonił nas do próby wypełnienia tej luki w piśmiennictwie polskim.

Ze względu na różnorodność zastosowań kombinatoryki książka nasza dzieli się wyraźnie na dwie części. Rozdział wstępny, w którym czynimy elementarny przegląd całej kombinatoryki, stanowi podstawę, na której opierają się wszystkie pozostałe rozdziały. Czytelnik poszukujący najprostszych informacji może zakończyć lekturę na tym rozdziale. Mimo to znajdzie w nim prawdopodobnie więcej informacji niż w dostępnych w języku polskim książkach Wilenkina [1] i Flachsmeyera [1]. Druga część zawierająca bardziej zaawansowane wyniki rozbija się w sposób naturalny na kilka działów. W pierwszym z nich przedstawiono zagadnienia związane z algebrą incydencji i funkcjami tworzącymi (rozdziały 2 i 3); decydujący wpływ na sposób przedstawienia przez nas materiału poświęconego tym zagadnieniom miał cykl prac G.-C. Roty i jego współpracowników pod wspólnym tytułem "On the foundations of combinatorial theory". Dalsza część książki poświęcona jest kolejno problematyce zagadnień minimaksowych (grupujących się wokół twierdzeń Halla i Dilwortha), następnie własnościom podziałowym (twierdzenia Ramseya, van der Waerdena, Halesa–Jewetta i inne). Następna część pracy składa się z rozdziałów dotyczących konfiguracji kombinatorycznych, kodów korygujących błędy oraz ciał skończonych. Rozdział 6, napisany przez M. Jaegermanna, poświęcony jest teorii zliczania Redfielda, Pólya i de Bruijna.

Książka nasza pomija wiele ważnych fragmentów kombinatoryki współczesnej, przede wszystkim teorię grafów; Czytelnik znajdzie tylko nieliczne wyniki związane z tą dziedziną. Pomijamy wreszcie ważną problematykę matroidów.

Konsekwencją przyjętego podziału książki na dwie części są nieliczne

powtórzenia w dalszym tekście materiału, który znajdował się we wstępie. Zyskała na tym, mamy nadzieję, ciągłość wykładu.

Książka ta nie powstałaby, gdyby nie pomoc licznych osób, które zachęcały nas do jej napisania: prof. dr. Jerzego Łosia, prof. dr. Zdzisława Pawlaka, doc. dr. Barbary Rokowskiej i innych. Oddzielne i specjalne podziękowania należą się dr. Michałowi Jaegermannowi. Ciągła z nim współpraca pomogła nam uniknąć wielu błędów i usterek.

Część tej książki powstała, gdy pierwszy autor pracował na Uniwersytecie Stanu Illinois w Urbana-Champaign, drugi zaś w Wenezuelskim Instytucie Badań Naukowych w Caracas.

Witold Lipski
Instytut Podstaw Informatyki PAN
Wiktor Marek
Uniwersytet Warszawski

ROZDZIAŁ I

WPROWADZENIE DO KOMBINATORYKI

§ 1. Pojęcia wstępne

W niniejszym paragrafie przypomnimy pewne podstawowe pojęcia teoriomnogościowe. Nie należy w żadnym razie traktować go jako wykładu elementów teorii mnogości. Czytelnika zainteresowanego takim wykładem odsyłamy do odpowiednich podręczników (np. Rasiowa [1] lub Marek i Onyszkiewicz [1]). Naszym celem jest raczej ustalenie terminologii i oznaczeń.

Będziemy używali standardowych oznaczeń logicznych, takich jak spójniki logiczne: $\neg$ (*negacja*), $\vee$ (*alternatywa*), $\wedge$ (*koniunkcja*), $\Rightarrow$ (*implikacja*), $\Leftrightarrow$ (*równoważność*).

Zbiory będziemy na ogół oznaczali dużymi literami A, B, C, ..., *zbiór pusty* symbolem $\emptyset$. Będziemy pisali $x \in A$ lub $x \notin A$ w zależności od tego, czy x *jest elementem*, czy też *nie jest elementem* zbioru A, natomiast oznaczeń $A \subseteq B$, $A \nsubseteq B$, $A \subset B$ będziemy używali odpowiednio dla oznaczenia faktu, iż A jest *podzbiorem* zbioru B, A nie jest podzbiorem zbioru B, oraz A jest *podzbiorem właściwym* zbioru B (tzn. $A \subseteq B$ i $A \neq B$). Operacje teoriomnogościowe *sumy*, *przecięcia* i *różnicy* zbiorów A i B oznaczamy odpowiednio przez $A \cup B$, $A \cap B$, $A \setminus B$. Będziemy mieli do czynienia głównie ze zbiorami skończonymi. Każdy taki zbiór możemy określić przez wyliczenie jego elementów. Zbiór, którego elementami są $x_1, \ldots, x_n$ i tylko te elementy, oznaczamy przez $\{x_1, \ldots, x_n\}$. W szczególności $\{x\}$ jest zbiorem, którego jedynym elementem jest x. Będziemy też pisali $\{x \in X\colon P(x)\}$ (lub $\{x\colon P(x)\}$ jeśli jasne jest jaki zbiór X mamy na myśli) dla oznaczenia zbioru tych elementów zbioru X, które mają własność P.

Terminów *zbiór*, *rodzina*, *klasa* będziemy używali zamiennie. Terminu „rodzina" na ogół będziemy używali w odniesieniu do zbioru, którego elementami są zbiory, terminu „klasa" natomiast w przypadku zbioru, którego elementami są rodziny zbiorów. Jeśli $\mathscr{A}$ jest rodziną zbiorów, to definiujemy

$$\bigcup \mathscr{A} = \{x\colon \text{istnieje zbiór } B \in \mathscr{A} \text{ taki, że } x \in B\},$$

$$\bigcap \mathscr{A} = \{x\colon \text{dla każdego } B \in \mathscr{A}\ x \in B\}.$$

Jeśli f jest funkcją przeprowadzającą elementy zbioru X w zbiór Y, to piszemy $f\colon X \to Y$ (odwzorowanie to przedstawiamy też czasem jako $x \mapsto f(x)$). Dla dowolnego $x \in X$ element $f(x)$ nazywamy *obrazem elementu* x, podobnie dla dowolnego $A \subseteq X$ zbiór

$$f(A) = \{f(x)\colon x \in A\}$$

nazywamy *obrazem zbioru* A (oczywiście przez $\{f(x)\colon x \in A\}$ rozumiemy zbiór $\{y \in Y\colon$ istnieje element $x \in A$ taki, że $y = f(x)\}$). Podobnie dla dowolnego $y \in Y$ i dowolnego $B \subseteq Y$ zbiory

$$f^{-1}(y) = \{x \in X\colon f(x) = y\}, \qquad f^{-1}(B) = \{x \in X\colon f(x) \in B\}$$

nazywamy *przeciwobrazem* odpowiednio *elementu* y i *zbioru* B. Jeśli $f\colon X \to Y$, to $\mathscr{D}(f) = X$ nazywamy *dziedziną funkcji* f, zaś $\mathscr{R}(f) = f(X)$ *przeciwdziedziną funkcji* f. Jeżeli $f(x) \neq f(y)$ dla dowolnych $x, y \in X$, $x \neq y$, to f nazywamy *funkcją rożnowartościową*. Jeśli $\mathscr{R}(f) = Y$, to f nazywamy *funkcją z* X *na* Y. Funkcję z X na Y, która jest różnowartościowa, nazywamy *odwzorowaniem wzajemnie jednoznacznym zbioru* X *na zbiór* Y. Dowolne wzajemnie jednoznaczne odwzorowanie $f\colon X \to X$ nazywamy *permutacją zbioru* X. Jeśli $f\colon X \to Y$ oraz $A \subseteq X$, to przez $f \restriction A$ oznaczamy *ograniczenie funkcji* f *do zbioru* A, tzn. funkcję $g\colon A \to Y$ taką, że $g(x) = f(x)$ dla każdego $x \in A$. Zbiór wszystkich funkcji $f\colon X \to Y$ oznaczamy przez Y^X.

Jeśli $f\colon X \to Y$, $g\colon Y \to Z$, to definiujemy *złożenie* $gf\colon X \to Z$ funkcji f i g następująco:

$$gf(x) = g\big(f(x)\big).$$

Przez *funkcję identycznościową* na zbiorze X rozumiemy funkcję $f\colon X \to X$ taką, że $f(x) = x$ dla dowolnego $x \in X$.

Funkcję $f\colon I \to Y$ będziemy czasem oznaczali przez $\langle f_i \rangle_{i \in I}$, gdzie f_i oznacza $f(i)$. Jeśli f_i jest zbiorem dla każdego $i \in I$, to mówimy o *indeksowanej rodzinie zbiorów*. Jeśli $\langle A_i \rangle_{i \in I}$ jest indeksowaną rodziną zbiorów, to definiujemy

$$\bigcup_{i \in I} A_i = \{x\colon \text{istnieje } i \in I \text{ takie, że } x \in A_i\},$$

$$\bigcap_{i \in I} A_i = \{x\colon \text{dla każdego } i \in I \ x \in A_i\}.$$

W teorii mnogości dwa zbiory A, B uważamy za *równe* wtedy i tylko wtedy, gdy każdy element zbioru A należy do zbioru B i każdy element zbioru B należy do zbioru A. A więc na przykład $\{a, a, b\} = \{a, b\}$. W kombinatoryce wygodnie jest rozważać twory ogólniejsze od zbiorów, zwane *zbiorami z powtórzeniami*, w których każdy element występuje określoną liczbę razy. Możemy oznaczyć przez (a, a, b) zbiór z powtórzeniami, w którym element a występuje dwukrotnie, element b zaś jednokrotnie (zakładamy $a \neq b$). W życiu codziennym spotykamy się często z sytuacjami, które w naturalny sposób odpowiadają pewnym zbiorom z

powtórzeniami. Możemy na przykład mówić o zbiorze z powtórzeniami monet (lub banknotów) znajdujących się w pewnej portmonetce, zbiorze z powtórzeniami znaczków będących w posiadaniu pewnego filatelisty, zbiorze z powtórzeniami figur szachowych itd. Choć pojęcie to jest intuicyjnie oczywiste, pokażemy jak można je sformalizować w języku klasycznej teorii mnogości, tak by zbiory z powtórzeniami stały się „legalnymi" obiektami matematyki. Załóżmy w tym celu, że wszystkie rozpatrywane przez nas elementy należą do pewnego zbioru X. Wtedy każdy zbiór z powtórzeniami A (o elementach ze zbioru X) możemy reprezentować przez funkcję r_A, która każdemu elementowi $x \in X$ przyporządkowuje nieujemną liczbę całkowitą $r_A(x)$ zwaną *współczynnikiem repetycji* elementu x w zbiorze z powtórzeniami A. Na przykład dla zbioru z powtórzeniami białych figur szachowych współczynnik repetycji piona jest równy 8, skoczka 2, króla 1 itd. Powiemy, że element x występuje w zbiorze z powtórzeniami A s razy, jeśli $r_A(x) = s$. Zbiory — będziemy je czasem nazywali *zbiorami bez powtórzeń* — traktujemy jako szczególny przypadek zbiorów z powtórzeniami, w których każdy element występuje co najwyżej raz. Jeśli A jest zbiorem bez powtórzeń, to r_A jest po prostu *funkcją charakterystyczną* tego zbioru:

$$r_A(x) = \begin{cases} 1, & \text{jeśli } x \in A, \\ 0, & \text{jeśli } x \notin A. \end{cases}$$

Będziemy rozważali głównie zbiory z powtórzeniami skończone, tzn. takie, dla których współczynnik repetycji jest różny od zera tylko dla skończonej liczby różnych elementów. Każdy taki zbiór z powtórzeniami A będziemy reprezentowali przez ciąg jego elementów (ujętych w nawiasy okrągłe), w którym każdy element występuje tyle razy, ile wynosi jego współczynnik repetycji. Dla przykładu zbiór z powtórzeniami białych figur szachowych możemy zapisać następująco:

$$F = (k, h, w, w, s, s, g, g, p, p, p, p, p, p, p, p),$$

gdzie k, h, w, s, g, p oznaczają odpowiednio króla, hetmana, wieżę, skoczka, gońca i piona. Będziemy też używać krótszego oznaczenia

$$F = (1*k, 1*h, 2*w, 2*s, 2*g, 8*p).$$

Często zamiast „zbiór z powtórzeniami $(s_1 * x_1, \ldots, s_n * x_n)$" będziemy mówili po prostu „zbiór $(s_1 * x_1, \ldots, s_n * x_n)$" lub też „zbiór s_1 nierozróżnialnych elementów $x_1, \ldots, s_n$ nierozróżnialnych elementów x_n".

Działania $A \cup B$, $A \cap B$, $A \setminus B$, $A \dot{\cup} B$ definiujemy na zbiorach z powtórzeniami następująco:

$$r_{A \cup B}(x) = \max(r_A(x), r_B(x)),$$

$$r_{A \cap B}(x) = \min(r_A(x), r_B(x)),$$

$$r_{A \setminus B}(x) = \max(r_A(x) - r_B(x), 0),$$

$$r_{A \dot{\cup} B}(x) = r_A(x) + r_B(x).$$

Zauważmy, że jeśli A jest zbiorem bez powtórzeń, to równość

$$A = A_1 \dot{\cup} \ldots \dot{\cup} A_t$$

oznacza, że $A_1, \ldots, A_t$ są zbiorami bez powtórzeń, $A = A_1 \cup \ldots \cup A_t$ oraz $A_i \cap A_j = \emptyset$, $1 \leqslant i < j \leqslant t$. *Liczność zbioru* $A = (s_1 * x_1, \ldots, s_n * x_n)$ oznaczamy przez $|A|$ i definiujemy następująco:

$$|A| = \sum_{i=1}^{n} s_i$$

(oczywiście definicja ta stosuje się w szczególności do skończonych zbiorów bez powtórzeń). Jeśli $|A| = k$, to mówimy, że A jest *k-elementowy*.

Dla dowolnej funkcji $f\colon X \to Y$ zbiór z powtórzeniami $A = (f(x)\colon P(x))$ definiujemy podobnie jak zbiór $\{f(x)\colon P(x)\}$, z tym że

$$r_A(y) = |\{x \in X\colon P(x) \wedge y = f(x)\}|$$

dla każdego $y \in Y$. Na przykład jeśli $B = \{-2, -1, 0, 1, 2\}$, to

$$(b^2\colon b \in B) = (1 * 0, 2 * 1, 2 * 4),$$

$$\{b^2\colon b \in B\} = \{0, 1, 4\}.$$

Dla dowolnego zbioru z powtórzeniami A piszemy $x \in A$, jeśli $r_A(x) \geqslant 1$, oraz $B \subseteq A$, jeśli dla zbioru z powtórzeniami B mamy $r_B(x) \leqslant r_A(x)$ dla każdego x. W tym ostatnim przypadku mówimy, że B jest *podzbiorem zbioru z powtórzeniami A*. Definiujemy

$$\mathscr{P}(A) = \{B\colon B \subseteq A\}$$

oraz dla dowolnej nieujemnej liczby całkowitej k

$$\mathscr{P}_k(A) = \{B\colon B \subseteq A \wedge |B| = k\}.$$

Zauważmy, że jeśli $B \subseteq A = (s_1 * x_1, \ldots, s_n * x_n)$, to

$$0 \leqslant r_B(x_1) \leqslant s_1, \ \ldots, \ 0 \leqslant r_B(x_n) \leqslant s_n.$$

Jeśli współczynnik repetycji elementu x_1 możemy wybrać na $s_1 + 1$ sposobów, elementu x_2 na $s_2 + 1$ sposobów, itd., to

$$|\mathscr{P}(A)| = (s_1 + 1) \ldots (s_n + 1).$$

W szczególności, jeśli A jest zbiorem bez powtórzeń, to $|A| = n$, $s_1 = \ldots = s_n = 1$ i w konsekwencji

$$|\mathscr{P}(A)| = 2^{|A|}.$$

Dla dowolnego, niekoniecznie skończonego zbioru z powtórzeniami A piszemy $B \subseteq_{\text{fin}} A$, jeśli $B \subseteq A$ oraz B jest skończonym zbiorem z powtórzeniami (zauważmy, że nasza definicja zbioru z powtórzeniami dopuszcza nieskończenie wiele różnych elementów, z których każdy występuje w zbiorze skończoną liczbę

razy). Definiujemy również

$$\mathscr{P}_{\text{fin}}(A) = \{B\colon\ B \subseteq_{\text{fin}} A\}.$$

Przez *ciąg długości n* rozumiemy dowolną funkcję określoną na zbiorze $\{1, \ldots, n\}$. Ciąg c taki, że $c(i) = c_i$ dla $1 \leqslant i \leqslant n$ będziemy oznaczali przez $\langle c_1, \ldots, c_n\rangle$ lub $c_1, \ldots, c_n$, albo po prostu przez $c_1 \ldots c_n$. Podobnie *ciąg nieskończony* definiujemy jako dowolną funkcję określoną na zbiorze liczb naturalnych.

Warto porównać pojęcie ciągu, zbioru z powtórzeniami i zbioru bez powtórzeń. Jeśli założymy, że $a \neq b$, to wszystkie trzy ciągi

$$\langle a, b, a\rangle, \quad \langle a, a, b\rangle, \quad \langle a, b, b\rangle$$

są różne, natomiast

$$(a, b, a) = (a, a, b) \neq (a, b, b),$$

$$\{a, b, a\} = \{a, a, b\} = \{a, b, b\} = \{a, b\}.$$

W przypadku ciągów istotna była zarówno liczba wystąpień każdego z elementów jak i kolejność elementów, w przypadku zbiorów z powtórzeniami ważna była jedynie liczba wystąpień każdego z elementów, w przypadku zbiorów odgrywało rolę jedynie to, jakie elementy występują w zbiorze.

Iloczyn kartezjański ciągu zbiorów $A_1, \ldots, A_n$ definiujemy następująco:

$$A_1 \times \ldots \times A_n = \{\langle a_1, \ldots, a_n\rangle\colon\ a_1 \in A_1 \wedge \ldots \wedge a_n \in A_n\}$$

(stosujemy też oznaczenie A^n, gdy $A_1 = \ldots = A_n = A$). Ogólnie, jeśli $\langle A_i\rangle_{i\in I}$ jest dowolną indeksowaną rodziną zbiorów, to iloczyn kartezjański tej rodziny definiujemy jako zbiór wszystkich funkcji $\langle a_i\rangle_{i\in I}$ takich, że $a_i \in A_i$ dla każdego $i \in I$. Iloczyn ten oznaczamy przez

$$\underset{i\in I}{\times} A_i.$$

Ciąg długości 2 nazywamy *parą uporządkowaną*, zbiór dwuelementowy natomiast *parą nieuporządkowaną*. Tak więc $X \times X$ jest zbiorem par uporządkowanych elementów zbioru X, natomiast $\mathscr{P}_2(X)$ zbiorem par nieuporządkowanych elementów zbioru X. Jeśli f jest funkcją określoną na $X_1 \times \ldots \times X_n$, to zamiast $f(\langle x_1, \ldots, x_n\rangle)$ piszemy $f(x_1, \ldots, x_n)$.

Relacją n-argumentową o dziedzinach $A_1, \ldots, A_n$ nazywamy dowolny podzbiór $R \subseteq A_1 \times \ldots \times A_n$. Zamiast $\langle a_1, \ldots, a_n\rangle \in R$ będziemy również pisali $R(a_1, \ldots, a_n)$.

W przypadku $R \subseteq A \times A$ mówimy o *relacji binarnej* na zbiorze A, o *dziedzinie*

$$\mathscr{D}(R) = \{a \in A\colon \text{ istnieje } b \in A \text{ takie, że } \langle a, b\rangle \in R\}$$

i *przeciwdziedzinie*

$$\mathscr{R}(R) = \{b \in A\colon \text{ istnieje } a \in A \text{ takie, że } \langle a, b\rangle \in R\}.$$

W przypadku relacji binarnej zamiast $\langle a, b\rangle \in R$ będziemy również pisali aRb. Dla dowolnego $B \subseteq A$ relację $R \cap (B \times B)$ nazywamy *ograniczeniem relacji R do zbioru B* i oznaczamy przez $R \upharpoonright B$.

Relację binarną R na zbiorze A nazywamy

zwrotną, jeśli dla dowolnego $a \in A$

$$aRa;$$

symetryczną, jeśli dla dowolnych $a, b \in A$

$$aRb \Leftrightarrow bRa;$$

przechodnią, jeśli dla dowolnych $a, b, c \in A$

$$aRb \wedge bRc \Rightarrow aRc;$$

antysymetryczną, jeśli dla dowolnych $a, b \in A$

$$aRb \wedge bRa \Leftrightarrow a = b;$$

spójną, jeśli dla dowolnych $a, b \in A$

$$aRb \vee bRa.$$

Relację binarną $R \subseteq A \times A$, która jest zwrotna, symetryczna i przechodnia, nazywamy *relacją równoważności* na zbiorze A. Jeśli E jest relacją równoważności na zbiorze A oraz $a \in A$, to zbiór

$$[a]_E = \{b \in A\colon aEb\}$$

(zwykle zamiast $[a]_E$ piszemy $[a]$) nazywamy *klasą abstrakcji* elementu a (względem relacji E). Rodzina klas abstrakcji relacji E, tzn.

$$A/_E = \{[a]_E\colon a \in A\}$$

jest rodziną niepustych i parami rozłącznych podzbiorów zbioru A, których sumą jest cały zbiór A. Każdą rodzinę o tej własności nazywamy *podziałem* zbioru A. Zbiory tej rodziny nazywamy zwykle *blokami* podziału.

Przyporządkowanie każdej relacji równoważności E na zbiorze A podziału $A/_E$ oraz każdemu podziałowi $\pi = \{B_1, \ldots, B_k\}$ relacji równoważności $(B_1 \times B_1) \cup \ldots \cup (B_k \times B_k)$ definiuje wzajemnie jednoznaczną odpowiedniość między relacjami równoważności na zbiorze A i podziałami tego zbioru.

Innymi ważnymi przykładami relacji binarnych są relacje porządku częściowego, którym poświęcamy następny paragraf.

Grafem (*niezorientowanym*) nazywamy dowolną parę $G = \langle V, E\rangle$, gdzie $E \subseteq \mathscr{P}_2(V)$. Zbiór V nazywamy zbiorem *wierzchołków*, E zaś zbiorem *krawędzi*. O krawędzi $e = \{x, y\}$ mówimy, że jest *incydentna* z wierzchołkiem x i z wierzchołkiem y, lub że łączy x z y. Podobnie dowolną parę $G = \langle V, E\rangle$, gdzie $E \subseteq V \times V$, nazywamy *grafem zorientowanym* o zbiorze wierzchołków V i zbiorze krawędzi E. O krawędzi $\langle x, y\rangle \in E$ mówimy, że *prowadzi* od x do y, lub że *odchodzi* od x i *dochodzi* do y. Krawędź postaci $\langle x, x\rangle$ nazywamy *pętlą*. Przez *podgraf* grafu $G = \langle V, E\rangle$ rozumiemy dowolny graf $G' = \langle V', E'\rangle$, $V' \subseteq V$, $E' \subseteq E$

(zorientowany lub niezorientowany, w zależności od tego czy G jest zorientowany, czy niezorientowany). Podgraf grafu $G = \langle V, E\rangle$ *indukowany* przez zbiór $W \subseteq V$ definiujemy jako $G_W = \langle W, E \cap \mathscr{P}_2(W)\rangle$, jeśli G jest niezorientowany, lub $G_W = \langle W, E \cap (W \times W)\rangle$, jeśli G jest zorientowany. *Drogą* z x do y długości n w grafie $G = \langle V, E\rangle$ nazywamy dowolny ciąg $x_0, x_1, \ldots, x_n$ wierzchołków taki, że $x = x_0$, $y = x_n$ oraz $\{x_0, x_1\}, \{x_1, x_2\}, \ldots, \{x_{n-1}, x_n\} \in E$ (jeśli G jest niezorientowany) lub $\langle x_0, x_1\rangle, \langle x_1, x_2\rangle, \ldots, \langle x_{n-1}, x_n\rangle \in E$ (jeśli G jest zorientowany). Droga taka jest *elementarna*, jeśli ciąg $x_0, \ldots, x_n$ jest różnowartościowy, oraz *cyklem*, jeśli $x_0 = x_n$ (cykl ten jest *elementarny*, jeśli ciąg $x_0, \ldots, x_{n-1}$ jest różnowartościowy). Łatwo zauważyć, że jeśli $G = \langle V, E\rangle$ jest grafem niezorientowanym, to relacja binarna $\approx$ zdefiniowana na zbiorze V przez

$$x \approx y \Leftrightarrow \text{istnieje w } G \text{ droga z } x \text{ do } y$$

jest relacją równoważności. Grafy indukowane postaci G_A, gdzie A jest klasą abstrakcji relacji $\approx$, nazywamy *składowymi spójnymi* grafu. Podobnie definiujemy składowe spójne grafu zorientowanego $G = \langle V, E\rangle$, z tym że w takim przypadku naszą relację równoważności definiujemy przez

$$x \approx y \Leftrightarrow \text{istnieje w } \tilde{G} \text{ droga z } x \text{ do } y,$$

gdzie $\tilde{G} = \langle V, \tilde{E}\rangle$, $\tilde{E} = \{\{a, b\}\colon \langle a, b\rangle \in E \wedge a \neq b\}$. Jeśli graf składa się z jednej składowej spójnej, to nazywamy go *spójnym*.

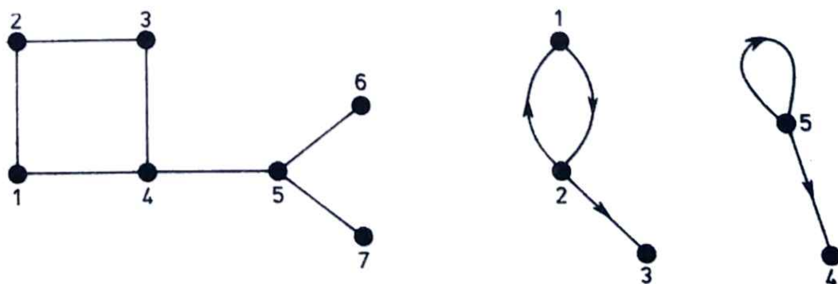
Będziemy mówili, że grafy $G_1 = \langle V_1, E_1\rangle$ i $G_2 = \langle V_2, E_2\rangle$ (oba niezorientowane lub oba zorientowane) są *izomorficzne*, jeśli istnieje wzajemnie jednoznaczne odwzorowanie $\varphi\colon V_1 \to V_2$ takie, że

$$\{x, y\} \in E_1 \Leftrightarrow \{\varphi(x), \varphi(y)\} \in E_2 \qquad (G_1, G_2 \text{ niezorientowane})$$

lub

$$\langle x, y\rangle \in E_1 \Leftrightarrow \langle \varphi(x), \varphi(y)\rangle \in E_2 \qquad (G_1, G_2 \text{ zorientowane}).$$

Grafy przedstawiamy zwykle za pomocą rysunku, na którym wierzchołkom odpowiadają punkty płaszczyzny, a krawędziom linie ciągłe łączące te punkty, z ewentualnie zaznaczoną orientacją (p. rys. 1).



Rys. 1 (a) Graf niezorientowany (spójny), (b) Graf zorientowany (niespójny)

$G = \langle V, E\rangle$ $\quad$ $G = \langle V, E\rangle$

$V = \{1, \ldots, 7\}$ $\quad$ $V = \{1, \ldots, 5\}$

$E = \{\{1, 2\}, \{2, 3\}, \{3, 4\}, \{1, 4\}, \{4, 5\}, \{5, 6\}, \{5, 7\}\}$ $\quad$ $E = \{\langle 1, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 5, 4\rangle, \langle 5, 5\rangle\}$

Graf niezorientowany, w którym każda para różnych wierzchołków jest połączona krawędzią, nazywamy *grafem pełnym*. Graf taki, o n wierzchołkach, oznaczamy zwykle przez K_n.

Poniżej podajemy niektóre oznaczenia często występujące w tekście:

N – zbiór liczb naturalnych 1, 2, ... (0 nie uważamy za liczbę naturalną),
N_0 $= N \cup \{0\}$,
Z – zbiór liczb całkowitych,
R – zbiór liczb rzeczywistych,
R^+ – zbiór liczb rzeczywistych nieujemnych,
C – zbiór liczb zespolonych,
$\lfloor x \rfloor$ – największa liczba całkowita mniejsza lub równa liczbie rzeczywistej x ($\lfloor 2\frac{1}{2} \rfloor = 2$, $\lfloor 3 \rfloor = 3$, $\lfloor -2\frac{1}{2} \rfloor = -3$),
$\lceil x \rceil$ – najmniejsza liczba całkowita większa lub równa liczbie rzeczywistej x ($\lceil 2\frac{1}{2} \rceil = 3$, $\lceil 3 \rceil = 3$, $\lceil -2\frac{1}{2} \rceil = -2$).

Wspomnimy jeszcze o pewnej konwencji – szczególnie często stosowanej w rozdziale 2 – dotyczącej jawnego wskazywania wskaźnika sumowania. Jeśli $P(i)$ jest pewną formułą zawierającą i, to

$$\sum_{i:P(i)} f(i)$$

oznacza sumę wszystkich $f(i)$ dla i przebiegającego zbiór $\{i: P(i)\}$.

§ 2. Zbiory częściowo uporządkowane

Pojęcie zbioru częściowo uporządkowanego odgrywa w kombinatoryce rolę podstawową. Wiele własności kombinatorycznych jest ściśle związanych z porządkiem wśród rozpatrywanych obiektów, i zbadanie struktury niektórych spośród tych porządków stanowi jedno z centralnych zagadnień kombinatoryki. W niniejszym paragrafie podamy ogólne definicje i fakty dotyczące zbiorów częściowo uporządkowanych.

Niech X będzie dowolnym zbiorem. Relację binarną $\leqslant$ na X nazywamy *częściowym porządkiem* (lub krótko *porządkiem*), jeśli jest ona zwrotna, przechodnia i antysymetryczna, tzn. jeśli

$$x \leqslant x,$$

$$x \leqslant y \wedge y \leqslant z \Rightarrow x \leqslant z,$$

$$x \leqslant y \wedge y \leqslant x \Rightarrow x = y$$

dla dowolnych $x, y, z \in X$. Parę $\langle X, \leqslant \rangle$, gdzie $\leqslant$ jest częściowym porządkiem na X, nazywamy *zbiorem częściowo uporządkowanym*. Częstokroć, jeśli wiadomo o jaką relację $\leqslant$ chodzi, sam zbiór X nazywamy zbiorem częściowo uporządkowanym. Jeśli $x \leqslant y$ lub $y \leqslant x$, to mówimy, że elementy x, y są *porównywalne*. Jeśli dowolne dwa elementy $x, y \in X$ są porównywalne, tzn. jeśli $\leqslant$ jest relacją spójną,

to $\leqslant$ nazywamy *porządkiem liniowym*, $\langle X, \leqslant\rangle$ zaś — *zbiorem liniowo uporządkowanym*. Łatwo zauważyć, że dla dowolnego zbioru częściowo uporządkowanego $\langle X, \leqslant\rangle$ i dowolnego $Y \subseteq X$ ograniczenie relacji $\leqslant$ do zbioru Y jest również częściowym porządkiem (zwykle oznaczamy go tym samym symbolem $\leqslant$, co nie prowadzi do nieporozumień). Jeśli $x \leqslant y$ i $x \neq y$, to piszemy $x < y$; zamiast $x \leqslant y$, $x < y$ piszemy również $y \geqslant x$, $y > x$. Element $x \in X$ nazywamy

minimalnym, jeśli nie istnieje element $y \in X$ taki, że $y < x$,

maksymalnym, jeśli nie istnieje element $y \in X$ taki, że $y > x$,

najmniejszym, jeśli $x \leqslant y$ dla każdego $y \in X$,

największym, jeśli $x \geqslant y$ dla każdego $y \in X$.

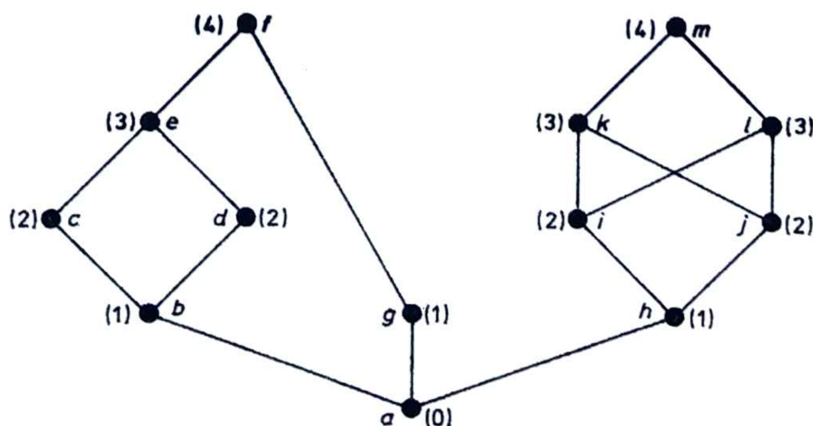
Element najmniejszy i największy nazywamy też *zerem* i *jedynką* zbioru częściowo uporządkowanego i oznaczamy zwykle przez 0 i 1. Oczywiście nie każdy zbiór częściowo uporządkowany ma zero i jedynkę, natomiast zero, jeśli istnieje, jest jedynym elementem minimalnym; podobnie jedynka jest jedynym elementem maksymalnym. Element minimalny (maksymalny itd.) podzbioru $Y \subseteq X$ definiujemy jako element minimalny (maksymalny itd.) w $\langle Y, \leqslant\rangle$. Jeśli $x < y$ i dla dowolnego $z \in X$

$$x \leqslant z \leqslant y \Rightarrow z = x \vee z = y$$

(gdzie $x \leqslant z \leqslant y$ jest skrótem dla $(x \leqslant z) \wedge (z \leqslant y)$), to mówimy, że y jest *bezpośrednim następnikiem* elementu x (x natomiast jest *bezpośrednim poprzednikiem* elementu y) i piszemy $x \lessdot y$.

Wygodnym sposobem reprezentacji skończonego zbioru częściowo uporządkowanego jest graf zorientowany zwany *diagramem Hassego*. Składa się on z wierzchołków odpowiadających elementom $x \in X$, przy czym $\langle x, y\rangle$ jest krawędzią grafu wtedy i tylko wtedy, gdy $x \lessdot y$. Na ogół nie zaznaczamy orientacji krawędzi diagramu Hassego, przyjmując, że jeśli $x \lessdot y$, to wierzchołek y znajduje się na diagramie wyżej niż wierzchołek x. Oczywiście $x \leqslant y$ wtedy i tylko wtedy, gdy w diagramie Hassego istnieje droga z x do y.

Zilustrujemy teraz wprowadzone pojęcia na przykładzie zbioru częściowo uporządkowanego, którego diagram Hassego przedstawiono na rys. 2. Nasz zbiór



Rys. 2. Diagram Hassego zbioru częściowo uporządkowanego

składa się z elementów $a, b, \ldots, m$. Elementy b, f są porównywalne, gdyż $b \leqslant f$, natomiast elementy b, g, czy też b, m, nie są porównywalne. Element a jest elementem minimalnym, natomiast f, m są elementami maksymalnymi. Nasz zbiór ma zero — jest nim element a — nie ma natomiast jedności.

Niech $\langle X, \leqslant \rangle$ będzie dowolnym zbiorem częściowo uporządkowanym i niech $Y \subseteq X$. Jeśli każde dwa elementy $x, y \in Y$ są porównywalne, tzn. jeśli porządek $\leqslant$ ograniczony do zbioru Y jest porządkiem liniowym, to Y nazywamy *łańcuchem*. Jeśli żadne dwa różne elementy $x, y \in Y$ nie są porównywalne, to Y nazywamy *antyłańcuchem*. Dla zbioru przedstawionego na rys. 2 przykładami łańcuchów są $\{a, j, k, m\}$, $\{a, b, d\}$, $\{a, f\}$, $\{d\}$, przykładami antyłańcuchów są natomiast $\{f, i, j\}$, $\{b, k, l\}$, $\{c, d, g, k, l\}$. Dla dowolnego skończonego niepustego łańcucha L przez jego *początek* i *koniec* rozumiemy element najmniejszy i największy zbioru L, *długość* zaś tego łańcucha definiujemy jako $|L|-1$. Przez *łańcuch maksymalny* między a i b rozumiemy łańcuch o początku a i końcu b, nie będący podzbiorem właściwym żadnego łańcucha o początku a i końcu b. Na rys. 2 łańcuchami maksymalnymi między a i f są

$$\{a, g, f\}, \quad \{a, b, d, e, f\}, \quad \{a, b, c, e, f\}.$$

Widzimy, że te łańcuchy są różnej długości (odpowiednio 2, 4 i 4). Jeśli dla dowolnych a, b wszystkie łańcuchy maksymalne między a i b są tej samej długości (zależnej od a, b), to mówimy, że zbiór częściowo uporządkowany spełnia *warunek Jordana–Dedekinda*.

Ważnym przykładem zbioru częściowo uporządkowanego jest dowolna rodzina $\mathscr{A} \subseteq \mathscr{P}(X)$ uporządkowana przez inkluzję, tzn. $\langle \mathscr{A}, \subseteq \rangle$. Pozostawiamy Czytelnikowi sprawdzenie, że jest to istotnie porządek częściowy. Okazuje się, że w pewnym sensie każdy zbiór częściowo uporządkowany jest postaci $\langle \mathscr{A}, \subseteq \rangle$. Aby to stwierdzenie uściślić, wprowadzimy następującą definicję. Dwa zbiory częściowo uporządkowane $\langle X_1, \leqslant_1 \rangle$ i $\langle X_2, \leqslant_2 \rangle$ są *izomorficzne* (fakt ten zapisujemy $\langle X_1, \leqslant_1 \rangle \simeq \langle X_2, \leqslant_2 \rangle$), jeśli istnieje wzajemnie jednoznaczne odwzorowanie f zbioru X_1 na zbiór X_2 takie, że dla dowolnego $x, y \in X_1$

$$x \leqslant_1 y \Leftrightarrow f(x) \leqslant_2 f(y).$$

Mamy następujące twierdzenie o reprezentacji:

TWIERDZENIE 2.1. *Każdy zbiór częściowo uporządkowany $\langle X, \leqslant \rangle$ jest izomorficzny z pewnym zbiorem postaci $\langle \mathscr{A}, \subseteq \rangle$, $\mathscr{A} \subseteq \mathscr{P}(X)$.*

Dowód. Wprowadźmy oznaczenie

$$\Delta(x) = \{y \in X\colon\ y \leqslant x\}, \qquad x \in X,$$

i niech

$$\mathscr{A} = \{\Delta(x)\colon\ x \in X\}.$$

Oczywiście $\Delta(x) \neq \Delta(y)$ dla $x \neq y$, gdyż $\Delta(x) = \Delta(y)$ pociąga za sobą $x \leqslant y$ i $y \leqslant x$, czyli, na mocy antysymetrii, $x = y$. Możemy zatem określić wzajemnie jednoznaczne odwzorowanie $f\colon X \to \mathscr{A}$ następująco:

$$f(x) = \Delta(x).$$

Odwzorowanie to ustala izomorfizm $\langle X, \leqslant\rangle \simeq \langle \mathscr{A}, \subseteq\rangle$, gdyż oczywiście

$$x \leqslant y \Leftrightarrow \Delta(x) \subseteq \Delta(y). \ \square$$

Niech $\langle X, \leqslant\rangle$ będzie dowolnym zbiorem częściowo uporządkowanym i niech $x \in X$. Oznaczmy przez $\mathscr{L}_x$ rodzinę wszystkich łańcuchów o końcu x. Jeśli istnieje liczba naturalna n taka, że długość żadnego łańcucha $L \in \mathscr{L}_x$ nie przekracza n, to definiujemy *rangę* elementu x (w $\langle X, \leqslant\rangle$) jako największą długość łańcucha w $\mathscr{L}_x$:

$$r(x) = \max\{|L|-1\colon\ L \in \mathscr{L}_x\}.$$

W przeciwnym przypadku mówimy, że ranga elementu x jest *nieskończona*.

Oczywiście ranga każdego elementu minimalnego jest równa zeru. Elementy rangi 1 nazywamy *atomami*. Łatwo zauważyć, że element jest atomem wtedy i tylko wtedy, gdy jest bezpośrednim następnikiem elementu minimalnego. Na rys. 2 przy każdym elemencie umieszczono w nawiasie jego rangę. Szczególnie łatwo znaleźć rangę elementu, jeśli w naszym zbiorze istnieje zero i jest spełniony warunek Jordana–Dedekinda. Wtedy bowiem ranga dowolnego elementu x (jeśli jest skończona) jest równa długości dowolnego łańcucha maksymalnego o początku w 0 i końcu x. Niech L będzie takim łańcuchem i niech $x \lessdot y$. Wtedy $L \cup \{y\}$ jest oczywiście łańcuchem maksymalnym o początku w 0 i końcu x, a zatem

(2.1) $$x \lessdot y \Rightarrow r(y) = r(x)+1$$

(oczywiście fakt ten jest prawdziwy również dla elementów rangi nieskończonej, jeśli przyjąć $r(x) = \infty$, $\infty+1 = \infty$).

Odcinkiem w zbiorze częściowo uporządkowanym $\langle X, \leqslant\rangle$ nazywamy każdy zbiór postaci

$$[x, y] = \{z \in X\colon\ x \leqslant z \leqslant y\}, \qquad x, y \in X.$$

Większość zbiorów częściowo uporządkowanych, z którymi mamy do czynienia w kombinatoryce, ma tę własność, że każdy odcinek jest skończony. Zbiory o tej własności nazywamy *lokalnie skończonymi*. Zauważmy, że w zbiorze lokalnie skończonym z zerem każdy odcinek $[0, x]$ jest skończony, a więc ranga dowolnego elementu jest skończona.

Łatwo zauważyć, że dla dowolnego porządku częściowego $\leqslant$ na zbiorze X relacja $\leqslant^*$ zdefiniowana przez

$$x \leqslant^* y \Leftrightarrow y \leqslant x$$

jest również częściowym porządkiem na X. Nazywamy go *porządkiem dualnym do* $\leqslant$.

Jeśli $\langle X_i, \leqslant_i \rangle$, $i \in I$, są zbiorami częściowo uporządkowanymi, to w iloczynie kartezjańskim $\times_{i \in I} X_i$ możemy wprowadzić porządek częściowy w następujący sposób:

$$f \leqslant g \Leftrightarrow \text{dla każdego } i \in I \ f_i \leqslant_i g_i$$

dla dowolnych $f, g \in \times_{i \in I} X_i$ (pozostawiamy Czytelnikowi sprawdzenie, że jest to istotnie porządek częściowy).

Zbiór $\langle \times_{i \in I} X_i, \leqslant \rangle$ nazywamy *iloczynem kartezjańskim* zbiorów częściowo uporządkowanych $\langle X_i, \leqslant_i \rangle$, $i \in I$.

Zauważmy, że iloczyn kartezjański nieskończonej liczby zbiorów lokalnie skończonych na ogół nie jest lokalnie skończony. Na przykład, jeśli dla każdego $i \in N$ zbiór $\langle X_i, \leqslant_i \rangle$ jest zbiorem $\{0, 1\}$ z porządkiem naturalnym $0 < 1$, to iloczyn kartezjański zbiorów częściowo uporządkowanych (lokalnie skończonych) $\langle X_i, \leqslant_i \rangle$, $i \in N$, nie jest lokalnie skończony, gdyż odcinek $[\mathbf{0}, \mathbf{1}]$, gdzie $\mathbf{0} = \langle 0, 0, \ldots \rangle$, $\mathbf{1} = \langle 1, 1, \ldots \rangle$, zawiera wszystkie nieskończone ciągi zero-jedynkowe.

Załóżmy teraz, że każdy ze zbiorów $\langle X_i, \leqslant_i \rangle$, $i \in I$, ma zero (będziemy je oznaczali dla każdego $i \in I$ tym samym symbolem 0). Oznaczmy przez $\bigoplus_{i \in I} X_i$ zbiór tych elementów $f \in \times_{i \in I} X_i$, dla których zbiór

$$I_f = \{i \in I \colon f_i \neq 0\},$$

zwany *nośnikiem* elementu f, jest skończony. Zbiór częściowo uporządkowany $\langle \bigoplus_{i \in I} X_i, \leqslant \rangle$ nazywamy *sumą prostą* zbiorów częściowo uporządkowanych (z zerem) $\langle X_i, \leqslant_i \rangle$, $i \in I$.

TWIERDZENIE 2.2. *Suma prosta $\langle \bigoplus_{i \in I} X_i, \leqslant \rangle$ zbiorów częściowo uporządkowanych lokalnie skończonych jest lokalnie skończona.*

Dowód. Niech $f, g \in \bigoplus_{i \in I} X_i$ oraz $f \leqslant g$. Rozważmy odcinek $[f, g]$. Jeśli $f \leqslant g$, to oczywiście $I_f \subseteq I_g$. Łatwo zauważyć, że odcinek $[f, g]$ jest izomorficzny z iloczynem kartezjańskim $\times_{i \in I_g} [f_i, g_i]$, co wobec skończoności zbioru I_g i lokalnej skończoności zbiorów $\langle X_i, \leqslant_i \rangle$, $i \in I_g$, dowodzi twierdzenia. □

Niech $\langle X, \leqslant \rangle$ będzie dowolnym zbiorem częściowo uporządkowanym i niech $Y \subseteq X$. Element $a \in X$ nazywamy *ograniczeniem górnym* zbioru Y, jeśli $x \leqslant a$ dla każdego $x \in X$. Podobnie, element $b \in X$ nazywamy *ograniczeniem dolnym* zbioru Y, jeśli $b \leqslant x$ dla każdego $x \in X$. Oznaczmy przez $A(Y)$ i $B(Y)$ odpowiednio zbiór wszystkich ograniczeń górnych i dolnych zbioru Y. Jeśli w $A(Y)$ istnieje element najmniejszy, to nazywamy go *kresem górnym* zbioru Y (w $\langle X, \leqslant \rangle$) i oznaczamy przez $\sup Y$. Podobnie, jeśli w $B(Y)$ istnieje element największy, to nazywamy go *kresem dolnym* zbioru Y (w $\langle X, \leqslant \rangle$) i oznaczamy przez $\inf Y$. Zwykle używamy

oznaczeń $x \vee y = \sup\{x, y\}$, $x \wedge y = \inf\{x, y\}$. Na przykład dla zbioru częściowo uporządkowanego z rys. 2 mamy $b \vee g = f$, $c \vee d = e$, $i \wedge j = h$, $g \wedge e = a$, elementy i, j nie mają kresu górnego, podobnie jak g, k czy też f, m; elementy k, l nie mają kresu dolnego.

Zbiór częściowo uporządkowany $\langle X, \leqslant\rangle$, w którym dla każdej pary elementów $x, y \in X$ istnieje kres górny $x \vee y$ i kres dolny $x \wedge y$, nazywamy *kratą*. Kratę nazywamy *zupełną*, jeśli istnieje $\sup Y$ i $\inf Y$ dla dowolnego $Y \subseteq X$. Z definicji kresu dolnego i górnego wynika natychmiast, że w dowolnej kracie

$$x \leqslant y \Leftrightarrow x \wedge y = x \Leftrightarrow x \vee y = y.$$

Kratę $\langle X, \leqslant\rangle$ nazywamy *rozdzielną*, jeśli dla dowolnych $x, y, z \in X$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z),$$

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

Przykładem kraty rozdzielnej jest $\langle \mathscr{A}, \subseteq\rangle$, gdzie $\mathscr{A}$ jest dowolną rodziną zbiorów spełniającą warunek

$$A \cup B,\ A \cap B \in \mathscr{A} \text{ dla dowolnych } A, B \in \mathscr{A}.$$

Kratę taką nazywamy *kratą zbiorów*. W kracie takiej oczywiście $A \vee B = A \cup B$, $A \wedge B = A \cap B$.

Innym przykładem kraty rozdzielnej jest $\langle N, |\rangle$, gdzie $|$ jest relacją podzielności na zbiorze liczb naturalnych. W takim przypadku oczywiście $m \wedge n = (m, n)$ (największy wspólny podzielnik), $m \vee n = [m, n]$ (najmniejsza wspólna wielokrotność).

Będziemy mówili, że w dowolnej kracie z zerem i jedynką element y jest *dopełnieniem* elementu x, jeśli $x \wedge y = 0$ i $x \vee y = 1$. Jeśli krata jest rozdzielna, to każdy element może mieć co najwyżej jedno dopełnienie. Istotnie, jeśli y, y' są dopełnieniami elementu x, to

$$y' = y' \wedge 1 = y' \wedge (x \vee y) = (y' \wedge x) \vee (y' \wedge y) = 0 \vee (y' \wedge y) = y' \wedge y,$$

i podobnie $y = y' \wedge y$, a więc $y' = y$. W takim przypadku jedyne dopełnienie elementu x oznaczamy przez $-x$. Kratę rozdzielną, w której każdy element ma dopełnienie, nazywamy *algebrą Boole'a*. Typowym przykładem algebry Boole'a jest *ciało zbiorów*, tzn. dowolna niepusta rodzina $\mathscr{F}$ podzbiorów ustalonego zbioru X zamknięta ze względu na operacje dopełnienia, sumy i przecięcia. Można wykazać, że wszystkie algebry Boole'a są, z dokładnością do izomorfizmu, tej postaci (por. Rasiowa i Sikorski [1]).

Zbiór częściowo uporządkowany $\langle X, \leqslant\rangle$ nazywamy *ufundowanym*, jeśli każdy niepusty podzbiór $Y \subseteq X$ ma (co najmniej jeden) element minimalny. Ufundowany zbiór liniowo uporządkowany nazywamy *zbiorem dobrze uporządkowanym* lub *porządkiem dobrym*. Łatwo zauważyć, że zbiór $\langle X, \leqslant\rangle$ jest ufundowany wtedy i tylko wtedy, gdy nie zawiera nieskończonych ciągów malejących postaci

$x_1 > x_2 > \ldots$ Istotnie, jeśli taki ciąg istnieje, to $Y = \{x_1, x_2, \ldots\}$ nie ma elementu minimalnego. Z drugiej strony, załóżmy, że pewien zbiór $Y \subseteq X$ nie ma elementu minimalnego. Wybierzmy dowolny element x_1. Nie jest on minimalny, istnieje więc w Y element $x_2 < x_1$. Element x_2 również nie jest minimalny, istnieje więc w Y element $x_3 < x_2$ itd. Rozumowanie to prowadzi do wniosku, że zbiór Y zawiera ciąg nieskończony postaci $x_1 > x_2 > \ldots$

TWIERDZENIE 2.3 (Zasada indukcji dla ufundowanych zbiorów częściowo uporządkowanych). *Niech $\langle X, \leqslant \rangle$ będzie ufundowanym zbiorem częściowo uporządkowanym i niech $Y \subseteq X$ będzie podzbiorem spełniającym dla każdego $x \in X$ warunek*

(2.2) $$\{y \in X:\ y < x\} \subseteq Y \Rightarrow x \in Y.$$

Wtedy $Y = X$.

Dowód. Przypuśćmy, że $Y \neq X$, tzn. $X \setminus Y \neq \emptyset$. Niech x będzie dowolnym elementem minimalnym zbioru $X \setminus Y$. Wobec minimalności mamy oczywiście $\{y \in X:\ y < x\} \subseteq Y$ i na mocy warunku (2.2) wnioskujemy, że $x \in Y$. Tak więc założenie, iż $X \setminus Y \neq \emptyset$ doprowadziło nas do sprzeczności. □

Warto tu zauważyć, że jeśli x jest elementem minimalnym w $\langle X, \leqslant \rangle$, to warunek (2.2) implikuje $x \in Y$.

Jeśli jako zbiór $\langle X, \leqslant \rangle$ przyjmiemy w twierdzeniu 2.3 zbiór liczb naturalnych ze zwykłą relacją niewiększości – który oczywiście jest ufundowany – to otrzymamy znaną zasadę indukcji dla liczb naturalnych.

Łatwo zauważyć, że każdy lokalnie skończony porządek częściowy z zerem jest ufundowany. Istotnie, nie może w nim istnieć ciąg nieskończony $x_1 > x_2 > \ldots$, gdyż każdy element tego ciągu należy do odcinka $[0, x_1]$, a odcinek ten jest skończony. Podamy obecnie kilka prostych lecz użytecznych faktów dotyczących zbiorów ufundowanych.

TWIERDZENIE 2.4. *Iloczyn kartezjański dowolnej skończonej liczby ufundowanych porządków częściowych jest ufundowany.*

Dowód. Niech $\langle X, \leqslant \rangle$ będzie iloczynem kartezjańskim ufundowanych porządków częściowych $\langle X_i, \leqslant_i \rangle$, $i \in I$. Rozważmy dowolny podzbiór $Y \subseteq X$. Dla każdego $A \subseteq X$ oznaczmy przez $p_i(A)$ rzut zbioru A na i-tą oś, tzn. $p_i(A) = \{x_i:\ x \in A\}$. Oznaczmy $A_1 = Y$. Zbiór $Y_1 = p_1(A_1) \subseteq X_1$ zawiera pewien element minimalny a_1. Utwórzmy zbiory $A_2 = \{x \in A_1:\ x_1 = a_1\}$, $Y_2 = p_2(A_2) \subseteq X_2$. Zbiór Y_2 zawiera pewien element minimalny a_2. Powtarzając tę konstrukcję otrzymujemy ciąg $\langle a_1, \ldots, a_n \rangle \in X$, który jest oczywiście elementem minimalnym zbioru Y. □

W podobny sposób można wykazać, że suma prosta dowolnej rodziny ufundowanych porządków częściowych z zerem jest ufundowana (por. zad. 27).

Niech $\langle X_i, \leqslant_i \rangle$, $i = 1, \ldots, n$, będą dowolnymi zbiorami liniowo uporządko-

wanymi. Wyznaczają one następujący porządek liniowy $\leqslant$ — zwany *porządkiem leksykograficznym* — na zbiorze $X = \mathop{\times}\limits_{i=1}^{n} X_i$:

$$\langle x_1, \ldots, x_n \rangle \leqslant \langle y_1, \ldots, y_n \rangle \Leftrightarrow$$
$$\Leftrightarrow \langle x_1, \ldots, x_n \rangle = \langle y_1, \ldots, y_n \rangle \text{ lub istnieje } k \leqslant n \text{ takie, że } x_i = y_i$$
$$\text{dla } 1 \leqslant i < k \text{ oraz } x_k <_k y_k.$$

TWIERDZENIE 2.5. *Jeśli* $\langle X_i, \leqslant_i \rangle$, $i = 1, \ldots, n$, *są porządkami dobrymi, to porządek leksykograficzny na* $X = \mathop{\times}\limits_{i=1}^{n} X_i$ *jest porządkiem dobrym.*

Dowód. Podobnie jak w dowodzie twierdzenia 2.4 rozważamy dowolny podzbiór $Y \subseteq X$, wyodrębniamy z niego elementy o minimalnej pierwszej współrzędnej, spośród nich elementy o minimalnej drugiej współrzędnej itd. Łatwo sprawdzić, że po n krokach pozostaje nam element minimalny zbioru Y. □

Na zakończenie podamy twierdzenie dotyczące definicji indukcyjnych, które będzie istotne w następnym rozdziale.

TWIERDZENIE 2.6 (O definiowaniu przez indukcję w ufundowanych zbiorach częściowo uporządkowanych). *Niech* $\langle X, \leqslant \rangle$ *będzie ufundowanym zbiorem częściowo uporządkowanym,* Y *zaś dowolnym zbiorem. Oznaczmy*

$$\mathscr{P} = \bigcup_{x \in X} Y^{B_x},$$

gdzie $B_x = \{y \in X\colon\ y < x\}$. *Dla każdej funkcji*

$$h\colon\ \mathscr{P} \to Y$$

istnieje dokładnie jedna funkcja $f\colon\ X \to Y$ *taka, że dla każdego* $x \in X$

$$f(x) = h(f \restriction B_x).$$

Zanim przystąpimy do dowodu tego twierdzenia wyjaśnimy jego intuicyjny sens. Funkcja h wyznacza regułę, która określa wartość definiowanej indukcyjnie funkcji dla elementu x na podstawie wartości funkcji dla wszystkich elementów $y < x$. Zauważmy, że jeśli x jest elementem minimalnym, to $B_x = \emptyset$, i ponieważ istnieje dokładnie jedna funkcja o dziedzinie pustej, funkcja h wyznacza jednoznacznie wartość definiowanej funkcji dla elementu x (wartość ta jest taka sama dla wszystkich elementów minimalnych; por. zad. 29). Równość $f(x) = h(f \restriction B_x)$ to właśnie bardzo ogólna postać definicji indukcyjnej.

Dowód twierdzenia 2.6. Wykażemy najpierw, że dla każdego elementu $x \in X$ istnieje co najwyżej jedna funkcja $g\colon\ \Delta(x) \to Y$, gdzie $\Delta(x) = B_x \cup \{x\}$, spełniająca warunek $g(y) = h(g \restriction B_y)$ dla każdego $y \leqslant x$. Istotnie, oznaczmy przez T zbiór tych $x \in X$, dla których istnieją co najmniej dwie takie funkcje.

Przypuśćmy, że $T \neq \emptyset$; wykażemy, że doprowadzi nas to do sprzeczności. Niech x będzie dowolnym elementem minimalnym zbioru T i niech $g_1, g_2\colon \Delta(x) \to Y$ będą dwiema różnymi funkcjami spełniającymi naszą definicję indukcyjną dla każdego $y \leqslant x$. Musi być $g_1 \upharpoonright B_x = g_2 \upharpoonright B_x$, gdyż $y \in T$ dla każdego $y < x$. Lecz również

$$g_1(x) = h(g_1 \upharpoonright B_x) = h(g_2 \upharpoonright B_x) = g_2(x),$$

czyli $g_1 = g_2$, co daje zapowiedzianą sprzeczność.

Niech teraz Z oznacza zbiór tych $x \in X$, dla których nie istnieje funkcja $g\colon \Delta(x) \to Y$ spełniająca warunek $g(y) = h(g \upharpoonright B_y)$ dla każdego $y \leqslant x$. Podobnie jak poprzednio przypuśćmy, że $Z \neq \emptyset$, i wybierzmy dowolny element minimalny x zbioru Z. Dla każdego $y < x$ istnieje wtedy funkcja $f_y\colon \Delta(y) \to Y$ spełniająca naszą definicję indukcyjną (oczywiście $f_y(z) = f_z(z)$ dla $z \leqslant y$). Niech $u\colon B_x \to Y$ będzie funkcją taką, że $u(y) = f_y(y)$ dla każdego $y < x$, i zdefiniujmy funkcję $f_x\colon \Delta(x) \to Y$ następująco:

$$f_x(y) = \begin{cases} u(y) & \text{dla } y < x, \\ h(u) & \text{dla } y = x. \end{cases}$$

Łatwo sprawdzić, że funkcja f_x spełnia naszą definicję indukcyjną dla każdego $y \leqslant x$, wbrew wyborowi x jako elementu zbioru Z. Sprzeczność ta dowodzi, iż musi być $Z = \emptyset$.

Wystarczy teraz przyjąć $f(x) = f_x(x)$ dla każdego $x \in X$. Wtedy

$$f(x) = f_x(x) = h(f_x \upharpoonright B_x) = h(f \upharpoonright B_x)$$

dla każdego $x \in X$. □

§ 3. Funkcje, permutacje, rozmieszczenia

Jednym z klasycznych zagadnień kombinatorycznych jest zadanie następującego typu. Mając dane zbiory X, Y, gdzie $|X| = n$, $|Y| = m$, znaleźć liczbę funkcji $f\colon X \to Y$ spełniających pewne ograniczenia. Tradycyjnie problem taki formułuje się jako pytanie o liczbę rozmieszczeń n obiektów w m pudełkach spełniających zadane warunki; „obiekt" $x \in X$ jest umieszczony w „pudełku" $y \in Y$ wtedy i tylko wtedy, gdy $f(x) = y$. Inną tradycyjną interpretację otrzymujemy traktując Y jako zbiór „kolorów", $f(x)$ natomiast jako „kolor elementu x". Wtedy każda funkcja $f\colon X \to Y$ odpowiada jednoznacznie pewnemu pokolorowaniu elementów zbioru X kolorami ze zbioru Y.

Najprostsza sytuacja jest oczywiście wtedy, gdy nie nakładamy żadnych ograniczeń na funkcję f.

TWIERDZENIE 3.1. *Jeśli* $|X| = n$ *i* $|Y| = m$, *to liczba funkcji* $f\colon X \to Y$ *jest równa* m^n.

Dowód. Bez zmniejszenia ogólności możemy przyjąć, że $X = \{1, \ldots, n\}$. Wtedy funkcje $f\colon X \to Y$ to nic innego jak ciągi długości n o wyrazach ze zbioru Y. Każdy spośród n wyrazów takiego ciągu możemy wybrać na m sposobów, wszystkich ciągów jest więc m^n. □

Łatwo jest również znaleźć liczbę rozmieszczeń, dla których w każdym pudełku znajduje się co najwyżej jeden obiekt. Mamy bowiem następujące twierdzenie.

TWIERDZENIE 3.2. *Jeśli* $|X| = n$ *i* $|Y| = m$, *to liczba funkcji różnowartościowych* $f\colon X \to Y$ *jest równa*

(3.1)
$$[m]_n = m(m-1)\ldots(m-n+1)$$

(*przyjmujemy* $[m]_0 = 1$).

Dowód. Podobnie jak poprzednio przyjmujemy $X = \{1, \ldots, n\}$, co sprowadza nasze zadanie do problemu znalezienia liczby ciągów różnowartościowych długości n. Załóżmy, że $n \leqslant m$. Wówczas pierwszy element ciągu możemy wybrać na m sposobów, drugi na $m-1$, i ogólnie, dla każdego wyboru pierwszych $i-1$ wyrazów, i-ty wyraz możemy wybrać na $m-(i-1) = m-i+1$ sposobów. Wszystkich takich ciągów długości n jest zatem $m(m-1)\ldots(m-n+1)$. Jeśli $n > m$, to oczywiście nie istnieje żadna funkcja różnowartościowa $f\colon X \to Y$, a jednocześnie jeden z czynników w (3.1) jest równy zeru. □

Uwaga. W starszej literaturze funkcje $f\colon \{1, \ldots, n\} \to Y$, gdzie $|Y| = m$, nazywane były *wariacjami n-wyrazowymi ze zbioru m-elementowego*, natomiast funkcje różnowartościowe $f\colon \{1, \ldots, n\} \to Y$ *wariacjami n-wyrazowymi ze zbioru m-elementowego bez powtórzeń.*

Jeśli $m = n$, to każda funkcja różnowartościowa $f\colon X \to Y$ jest funkcją z X na Y. W takim przypadku $[m]_n$ oznaczamy tradycyjnie przez $n!$ ($0! = 1$). Mamy więc

TWIERDZENIE 3.3. *Jeśli* $|X| = |Y| = n$, *to liczba odwzorowań wzajemnie jednoznacznych* $f\colon X \to Y$ *jest równa*

$$n! = n(n-1)\ldots 1.$$

W szczególności istnieje dokładnie $n!$ *permutacji zbioru n-elementowego.* □

Wyznaczenie liczby funkcji z X na Y odkładamy do paragrafu 7, obecnie natomiast zajmiemy się znalezieniem rozmieszczeń specjalnego typu, które nie podpadają bezpośrednio pod schemat funkcji spełniających pewne ograniczenia. Będziemy rozważali rozmieszczenia obiektów ze zbioru n-elementowego X w m pudełkach, przy czym zakładamy, że obiekty w każdym pudełku są uporządkowane w ciąg (pudełko może być puste). Dwa rozmieszczenia uważamy za identyczne wtedy i tylko wtedy, gdy w obu przypadkach zawierają w każdym

pudełku ten sam ciąg. Oto dla przykładu wszystkie 12 rozmieszczeń elementów *a*, *b* w trzech pudełkach:

a, *b*		
b, *a*		
a	*b*	
b	*a*	
	a, *b*	
	b, *a*	
	a	*b*
	b	*a*
a		*b*
b		*a*
		a, *b*
		b, *a*

Rozmieszczenia opisanego przez nas typu będziemy nazywali *rozmieszczeniami uporządkowanymi* elementów zbioru X w m pudełkach.

TWIERDZENIE 3.4. *Jeśli* $|X| = n$, *to liczba rozmieszczeń uporządkowanych elementów zbioru* X *w* m *pudełkach jest równa*

$$[m]^n = m(m+1)\dots(m+n-1) \tag{3.2}$$

($[m]^0 = 1$).

Dowód. Niech $X = \{x_1, \dots, x_n\}$. Będziemy rozmieszczali kolejno elementy $x_1, \dots, x_n$. Mamy dokładnie m możliwości rozmieszczenia elementu x_1 (tyle ile jest pudełek) i $m+1$ możliwości rozmieszczenia elementu x_2, gdyż możemy go rozmieścić w jednym spośród $m-1$ pustych pudełek oraz na dwa sposoby w pudełku zawierającym x_1 – przed x_1 lub za x_1. Ogólnie, załóżmy, że rozmieściliśmy już elementy $x_1, \dots, x_{k-1}$, przy czym w i-tym pudełku znajduje się

r_i elementów, $i = 1, \ldots, m$. Element x_k możemy rozmieścić w i-tym pudełku na r_i+1 sposobów, w sumie więc na

$$\sum_{i=1}^{m} (r_i+1) = m + \sum_{i=1}^{m} r_i = m+k-1$$

sposobów. Liczba wszystkich rozmieszczeń uporządkowanych elementów zbioru X w m pudełkach jest zatem równa $m(m+1)\ldots(m+n-1)$. □

§ 4. Rozkład permutacji na cykle, liczby Stirlinga pierwszego rodzaju

Oznaczmy przez S_n zbiór wszystkich permutacji zbioru $X = \{1, \ldots, n\}$. Dowolną permutację $f \in S_n$ będziemy oznaczali w następujący sposób:

(4.1) $$\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}.$$

Każdej takiej permutacji możemy przyporządkować graf zorientowany o zbiorze wierzchołków X i zbiorze krawędzi $E = \{\langle x, f(x)\rangle : x \in X\}$. Zauważmy, że w takim grafie od każdego wierzchołka odchodzi dokładnie jedna krawędź (gdyż f jest funkcją), oraz do każdego wierzchołka dochodzi dokładnie jedna krawędź (gdyż f jest funkcją różnowartościową). Wybierzmy dowolny element $x \in X$ i rozważmy ciąg $x_0 = x$, $x_1 = f(x_0)$, $x_2 = f(x_1)$, ... Niech x_k będzie pierwszym elementem tego ciągu o tej własności, że $x_k = x_l$ dla pewnego $l < k$. Mamy $l = 0$, gdyż w przeciwnym przypadku $f(x_{l-1}) = f(x_{k-1})$, $x_{l-1} \neq x_{k-1}$, wbrew różnowartościowości funkcji f. Stąd wniosek, że każda składowa spójna naszego grafu jest cyklem elementarnym. Przykład permutacji i odpowiadającego jej grafu pokazano na rys. 3. Permutację taką zapisujemy zwykle jako

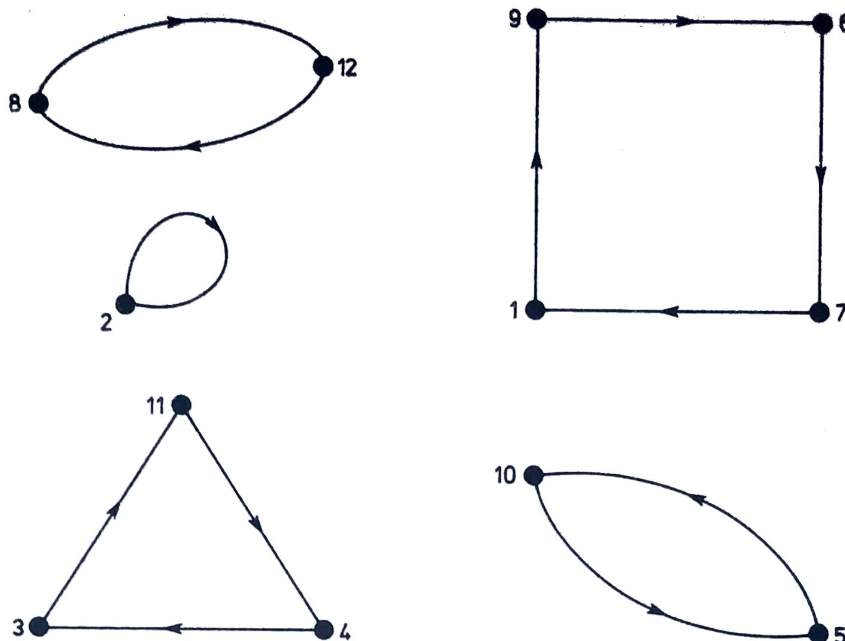
(4.2) $$f = [1\ 9\ 6\ 7]\ [3\ 1\ 4]\ [8\ 12]\ [5\ 10]\ [2].$$

Zapis taki nazywamy *rozkładem permutacji f na cykle*, lub *rozkładem kanonicznym* tej permutacji.

Zauważmy, że jeśli cykl $[a_0, \ldots, a_{k-1}]$ traktować jako permutację $\varphi \in S_n$, gdzie $\varphi(a_i) = a_{i+1 (\mathrm{mod}\, k)}$ oraz $\varphi(x) = x$ jeśli $x \notin \{a_0, \ldots, a_{k-1}\}$, to zapis (4.2) możemy traktować jako złożenie cykli. Kolejność w jakiej cykle występują w (4.1) jest nieistotna, gdyż żadne dwa cykle nie zawierają wspólnych elementów.

Będziemy mówili, że permutacja $f \in S_n$ jest *typu* $\langle \lambda_1, \ldots, \lambda_n \rangle$, jeśli w jej rozkładzie kanonicznym występuje λ_i cykli długości i dla $i = 1, 2, \ldots, n$. Tradycyjnie typ taki oznaczamy przez symboliczny zapis $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$. Oczywiście typ $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ każdej permutacji $f \in S_n$ spełnia warunek

$$\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n = n.$$



Rys. 3. Permutacja i jej rozkład kanoniczny

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 2 & 11 & 3 & 10 & 7 & 1 & 12 & 6 & 5 & 4 & 8 \end{pmatrix}$$

Każdą permutację typu n^1 (tzn. $1^0 2^0 \ldots n^1$) nazywamy *cykliczną.*

Można podać teoriogrupową charakteryzację permutacji tego samego typu. Aby to uczynić, wprowadźmy następującą definicję. Permutacje $f, g \in S_n$ nazywamy *sprzężonymi,* jeśli istnieje permutacja $h \in S_n$ taka, że $y = hfh^{-1}$.

TWIERDZENIE 4.1. *Permutacje f, g są sprzężone wtedy i tylko wtedy, gdy są tego samego typu.*

Dowód. Załóżmy, że $g = hfh^{-1}$ i niech

$$f = [a_0^{(1)} a_1^{(1)} \ldots a_{n_1-1}^{(1)}] [a_0^{(2)} a_1^{(2)} \ldots a_{n_2-1}^{(2)}] \ldots [a_0^{(k)} a_1^{(k)} \ldots a_{n_k-1}^{(k)}]. \tag{4.3}$$

Oznaczmy

$$h(a_i^{(j)}) = b_i^{(j)}, \qquad 1 \leqslant j \leqslant k, \ 0 \leqslant i < n_j. \tag{4.4}$$

Mamy wtedy

$$g(b_i^{(j)}) = hfh^{-1} h(a_i^{(j)}) = hf(a_i^{(j)}) = h(a_{i+1 (\mathrm{mod}\, n_j)}^{(j)}) = b_{i+1 (\mathrm{mod}\, n_j)}^{(j)},$$

co oznacza, że

$$g = [b_0^{(1)} b_1^{(1)} \ldots b_{n_1-1}^{(1)}] [b_0^{(2)} b_1^{(2)} \ldots b_{n_2-1}^{(2)}] \ldots [b_0^{(k)} b_1^{(k)} \ldots b_{n_k-1}^{(k)}]. \tag{4.5}$$

Tak więc f i g są tego samego typu.

Na odwrót, załóżmy, że f i g są tego samego typu. Wtedy f i g możemy zapisać odpowiednio w postaci (4.3) i (4.5). Zdefiniujmy permutację $h \in S_n$ wzorem (4.4). Mamy wtedy $g = hfh^{-1}$. □

Znajdźmy dla przykładu wszystkie permutacje $f \in S_4$ typu $1^1 3^1$. Łatwo sprawdzić, że jest ich osiem:

$$[1][2\ 3\ 4], \quad [1][2\ 4\ 3],$$
$$[2][1\ 3\ 4], \quad [2][1\ 4\ 3],$$
$$[3][1\ 2\ 4], \quad [3][1\ 4\ 2],$$
$$[4][1\ 2\ 3], \quad [4][1\ 3\ 2].$$

TWIERDZENIE 4.2 (Cauchy). *Liczba permutacji typu* $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ *zbioru n-elementowego* ($\lambda_1 + 2\lambda_2 + \dots + n\lambda_n = n$) *jest równa*

(4.6) $$h(\lambda_1, \dots, \lambda_n) = \frac{n!}{1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!}.$$

Dowód. Niech f będzie dowolną permutacją typu $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$. Zapis

(4.7) $$f = [a_0^{(1)} a_1^{(1)} \dots a_{n_1-1}^{(1)}] \dots [a_0^{(k)} a_1^{(k)} \dots a_{n_k-1}^{(k)}]$$

będziemy nazywali *znormalizowanym*, jeśli występuje w nim najpierw λ_1 cykli długości 1, potem λ_2 cykli długości 2 itd. Zauważmy, że w takim zapisie możemy – bez zmiany permutacji definiowanej przez ten zapis – zmieniać na $\lambda_i!$ sposobów porządek, w jakim występują cykle długości i, oraz każdy taki cykl przesuwać cyklicznie na i sposobów:

$$[a_0 a_1 \dots a_{i-1}] \to [a_1 a_2 \dots a_{i-1} a_0] \to \dots \to [a_{i-1} a_0 \dots a_{i-2}].$$

Widać stąd, że każda permutacja typu $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ jest definiowana przez $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n} \lambda_1! \lambda_2! \dots \lambda_n!$ zapisów znormalizowanych. Oczywiście dla ustalonego typu $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ wszystkich zapisów znormalizowanych postaci (4.7) jest tyle, ile wszystkich ciągów różnowartościowych długości n o elementach z $\{1, \dots, n\}$, tzn. $n!$. Liczba różnych permutacji typu $1^{\lambda_1} 2^{\lambda_2} \dots n^{\lambda_n}$ jest więc dana przez (4.6). □

Zajmiemy się teraz liczbą permutacji zbioru n-elementowego, które w rozkładzie kanonicznym mają dokładnie k cykli. Oznaczmy liczbę takich permutacji przez $c(n, k)$ (przyjmujemy $c(0, 0) = 1$).

TWIERDZENIE 4.3. *Liczby* $c(n, k)$ *spełniają zależności*

(4.8) $$c(n, k) = c(n-1, k-1) + (n-1)c(n-1, k), \quad 0 < k < n,$$

(4.9) $$c(n, n) = 1, \quad n \geqslant 0,$$

(4.10) $$c(n, 0) = c(0, k) = 0, \quad n, k > 0.$$

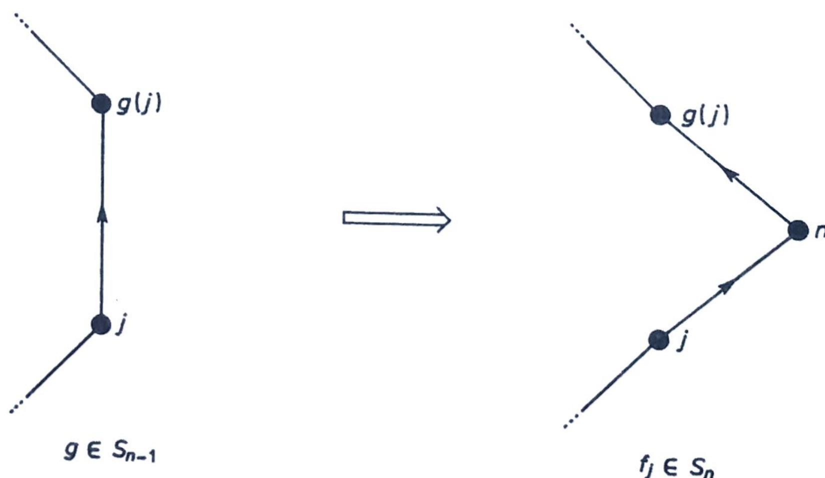
Dowód. Równość (4.9) wynika z faktu, iż jedyną permutacją mającą w rozkładzie kanonicznym n cykli jest permutacja identycznościowa. Równie oczywiste są równości (4.10). Załóżmy teraz, że $0 < k < n$. Permutacje $f \in S_n$ mające w rozkładzie kanonicznym k cykli możemy podzielić na dwie rozłączne klasy A i B. Do A zaliczymy te permutacje, dla których $f(n) = n$, tzn. te, dla których $[n]$ jest jednym z cykli. Permutacji takich jest oczywiście $c(n-1, k-1)$. Klasa B zawiera pozostałe permutacje, tzn. te, w których n występuje w cyklu długości większej od jedności. Zauważmy, że z każdej permutacji $f \in B$ możemy utworzyć permutację $g \in S_{n-1}$ o k cyklach, przyjmując

$$g(i) = \begin{cases} f(n), & \text{jeśli } f(i) = n, \\ f(i) & \text{w pozostałych przypadkach.} \end{cases}$$

Przy tej konstrukcji ta sama permutacja $g \in S_{n-1}$ o k cyklach powstaje z dokładnie $n-1$ permutacji $f_j \in B$, $1 \leqslant j \leqslant n-1$, gdzie

$$f_j(i) = \begin{cases} g(j), & \text{jeśli } i = n, \\ n, & \text{jeśli } i = j, \\ g(i), & \text{w pozostałych przypadkach} \end{cases}$$

(p. rys. 4). Stąd $|B| = (n-1)c(n-1, k)$, co dowodzi twierdzenia. □



Rys. 4. Rozszerzenie permutacji $g \in S_{n-1}$ do permutacji $f_j \in S_n$ (p. dowód twierdzenia 4.3)

Rozważmy teraz, przez analogię do wzoru (3.1), następujące wyrażenie:

$$[x]_n = x(x-1)\ldots(x-n+1).$$

Określa ono pewien wielomian zmiennej x stopnia n o współczynnikach całkowitych, możemy więc napisać

$$[x]_n = \sum_{i=0}^{n} s(n, k)x^k. \tag{4.11}$$

Określone w ten sposób liczby $s(n, k)$ zwane są *liczbami Stirlinga pierwszego rodzaju* (przyjmujemy $s(n, k) = 0$ dla $k > n$, oraz $s(0, 0) = 1$, co jest konsekwencją umowy $[x]_0 = 1$). Liczby $s(n, k)$ dla $0 \leqslant n, k \leqslant 10$ przedstawiono w tabl. 1.

Tablica 1. Liczby Stirlinga pierwszego rodzaju $s(n, k)$

$n \backslash k$	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0
2	0	−1	1	0	0	0	0	0	0	0	0
3	0	2	−3	1	0	0	0	0	0	0	0
4	0	−6	11	−6	1	0	0	0	0	0	0
5	0	24	−50	35	−10	1	0	0	0	0	0
6	0	−120	274	−225	85	−15	1	0	0	0	0
7	0	720	−1764	1624	−735	175	−21	1	0	0	0
8	0	−5040	13068	−13132	6769	−1960	322	−28	1	0	0
9	0	40320	−109584	118124	−67284	22449	−4536	546	−36	1	0
10	0	−362880	1026576	−1172700	723680	−269325	63273	−9450	870	−45	1

Wartości liczb $s(n, k)$ łatwo obliczać korzystając z następującego twierdzenia.

TWIERDZENIE 4.4. *Liczby Stirlinga pierwszego rodzaju spełniają zależności*

$$s(n, k) = s(n-1, k-1) - (n-1)s(n-1, k), \qquad 0 < k < n, \tag{4.12}$$

$$s(n, n) = 1, \qquad n \geqslant 0, \tag{4.13}$$

$$s(n, 0) = s(0, k) = 0, \qquad n, k > 0. \tag{4.14}$$

Dowód. Równości (4.13), (4.14) są oczywiste, niech więc $0 < k < n$. Mamy wtedy

$$[x]_n = [x]_{n-1}(x-n+1),$$

a stąd

$$\sum_{k=0}^{n} s(n, k)x^k = (x-n+1)\sum_{k=0}^{n-1} s(n-1, k)x^k =$$

$$= \sum_{k=1}^{n} s(n-1, k-1)x^k - (n-1)\sum_{k=0}^{n-1} s(n-1, k)x^k.$$

Równość (4.12) otrzymujemy teraz przez porównanie współczynników przy x^k $(0 < k < n)$. □

Z twierdzeń 4.3 i 4.4 wynika już łatwo, że wartość bezwzględna liczby $s(n, k)$ jest równa liczbie permutacji zbioru n-elementowego o k cyklach w rozkładzie kanonicznym.

TWIERDZENIE 4.5. *Dla dowolnych $n, k \geqslant 0$*

$$c(n, k) = |s(n, k)| = (-1)^{n+k} s(n, k). \tag{4.15}$$

D o w ó d. Oznaczmy $a(n, k) = (-1)^{n+k} s(n, k)$. Mamy wtedy

$$a(n, n) = (-1)^{2n} s(n, n) = 1 = c(n, n), \qquad n \geqslant 0,$$

$$a(n, 0) = a(0, k) = (-1)^n s(n, 0) = (-1)^k s(0, k) =$$
$$= 0 = c(n, 0) = c(0, k), \qquad n, k > 0,$$

oraz dla $0 < k < n$

$$a(n, k) = (-1)^{n+k} s(n, k) =$$
$$= (-1)^{n+k} s(n-1, k-1) - (-1)^{n+k} (n-1) s(n-1, k) =$$
$$= (-1)^{(n-1)+(k-1)} s(n-1, k-1) + (-1)^{(n-1)+k} (n-1) s(n-1, k) =$$
$$= a(n-1, k-1) + (n-1) a(n-1, k).$$

Widać stąd, że liczby $a(n, k)$ spełniają te same zależności rekurencyjne i te same warunki początkowe, co liczby $c(n, k)$ (p. twierdzenie 4.3). Tak więc $a(n, k) = c(n, k)$ dla dowolnych $n, k \geqslant 0$ (szczegółowy dowód tego faktu przez indukcję względem $n+k$ pozostawiamy Czytelnikowi). □

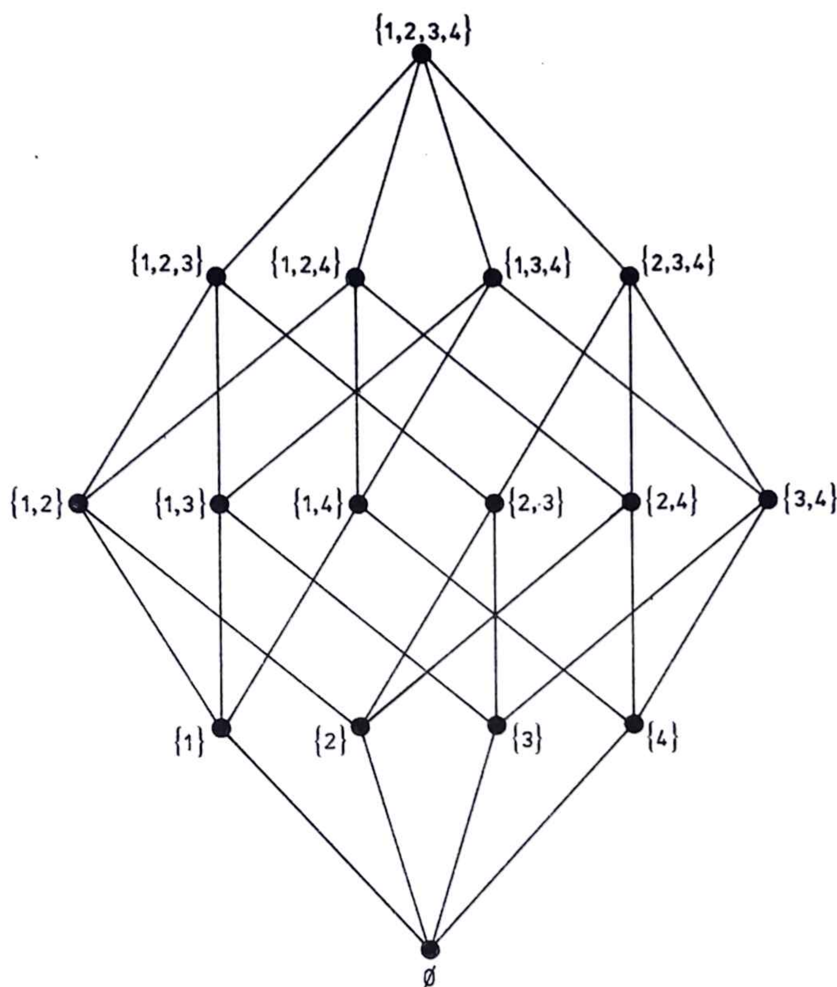
Ze względu na wzór (4.15) liczby $c(n, k)$ są czasem nazywane *nieoznakowanymi liczbami Stirlinga pierwszego rodzaju*. Liczby $s(n, k)$ mają wiele ciekawych własności. Będziemy do nich jeszcze powracali.

§ 5. Kombinacje, współczynnik dwumienny

Zajmiemy się teraz strukturą zbioru częściowo uporządkowanego $\langle \mathscr{P}(X), \subseteq \rangle$, gdzie X jest zbiorem n-elementowym (p. rys. 5). Porządek ten jest oczywiście wyznaczony z dokładnością do izomorfizmu przez $n = |X|$, zatem bez zmniejszenia ogólności zakładamy zwykle $X = \{1, \ldots, n\}$. W $\langle \mathscr{P}(X), \subseteq \rangle$ istnieje zero i jedność, są nimi odpowiednio $\emptyset$ i X. Łatwo również zauważyć, że ranga elementu $A \in \mathscr{P}(X)$ to nic innego jak liczność zbioru A:

$$r(A) = |A|.$$

Jednym z najprostszych, a jednocześnie ważnych z kombinatorycznego punktu widzenia pytań dotyczących struktury porządku częściowego jest pytanie o liczbę elementów rangi k. W naszym przypadku pytamy o liczbę podzbiorów k-elementowych zbioru n-elementowego. Podzbiory takie są czasem nazywane tradycyjnie *kombinacjami k-wyrazowymi ze zbioru n-elementowego bez powtórzeń*, a ich liczba jest oznaczana przez $\binom{n}{k}$ (używane są też czasem oznaczenia $C(n, k)$, C_k^n,



Rys. 5. Częściowy porządek $\langle \mathscr{P}(X), \subseteq \rangle$, $X = \{1, 2, 3, 4\}$

${}_nC_k$). Symbol $\binom{n}{k}$ zwany jest *symbolem Newtona* lub *współczynnikiem dwumiennym*, ze względu na następujący wzór na n-tą potęgę dwumianu podany przez Newtona w roku 1676:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}. \tag{5.1}$$

Wzór ten staje się oczywisty, jeśli zauważymy, że współczynnik przy $x^k y^{n-k}$ w rozwinięciu iloczynu $(x+y)\dots(x+y)$ jest równy liczbie sposobów, jakimi spośród n czynników $x+y$ można wybrać k nawiasów jako te, z których wybieramy składnik x. Łatwo zauważyć, że wzór ten jest prawdziwy w dowolnym pierścieniu przemiennym, a nawet w zupełnie dowolnym pierścieniu, jeśli $xy = yx$ (np. gdy $x = 1$).

Zauważmy, że $\binom{n}{k} = 0$ dla $k > n \geqslant 0$. W dalszym ciągu będziemy zakładali, że

liczby pojawiające się we współczynnikach Newtona są całkowite nieujemne (założenie to, dla górnego wskaźnika, potem osłabimy).

Znana jest olbrzymia liczba tożsamości związanych ze współczynnikami dwumiennymi (p. np. Riordan [1, 2], Kaucký [1]). Podamy obecnie parę prostych przykładów.

Zliczając podzbiory zbioru n-elementowego według ich liczności, innymi słowy korzystając z faktu, iż $\mathscr{P}(X) = \mathscr{P}_0(X) \dot{\cup} \mathscr{P}_1(X) \dot{\cup} \ldots \dot{\cup} \mathscr{P}_n(X)$, otrzymujemy

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \tag{5.2}$$

(inny prosty dowód polega na podstawieniu $x = y = 1$ w (5.1)). Odwzorowanie $f(A) = X \setminus A$ ustala odpowiedniość wzajemnie jednoznaczną między podzbiorami k-elementowymi a podzbiorami $(n-k)$-elementowymi zbioru n-elementowego X, zatem

$$\binom{n}{k} = \binom{n}{n-k}, \qquad k \leqslant n. \tag{5.3}$$

To samo odwzorowanie ustala odpowiedniość wzajemnie jednoznaczną między podzbiorami o liczności parzystej a podzbiorami o liczności nieparzystej, jeśli n jest nieparzyste. W przypadku n parzystego wystarczy zauważyć, że istnieje tyle samo podzbiorów o liczności parzystej co i nieparzystej, zawierających pewien ustalony element, jak również tyle samo podzbiorów o liczności parzystej co i nieparzystej, nie zawierających tego elementu. Otrzymujemy stąd tożsamość

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0, \tag{5.4}$$

którą można również udowodnić podstawiając $x = 1$, $y = -1$ do wzoru (5.1).

Wykażemy teraz *tożsamość Cauchy'ego*

$$\binom{m+n}{k} = \sum_{r=0}^{k} \binom{n}{r}\binom{m}{k-r}. \tag{5.5}$$

W tym celu obliczymy na dwa sposoby liczbę podzbiorów k-elementowych zbioru $(n+m)$-elementowego $M \cup N$, gdzie $|M| = m$, $|N| = n$, $M \cap N = \emptyset$. Wszystkie k-elementowe zbiory $K \subseteq M \cup N$ możemy podzielić na grupy rozłączne według parametru $r = |K \cap N|$. Każdy podzbiór K w takiej grupie możemy utworzyć wybierając najpierw r-elementowy podzbiór $A \subseteq N$ $(A = K \cap N)$, a następnie $(k-r)$-elementowy podzbiór $B \subseteq M$ $(B = K \cap M)$. Podzbiór A możemy wybrać na $\binom{n}{r}$ sposobów, podzbiór B zaś na $\binom{m}{k-r}$ sposobów, liczność naszej grupy wynosi zatem $\binom{n}{r}\binom{m}{k-r}$. Parametr r może przyjmować wartości $0, 1, \ldots, k$, co daje

ostatecznie wzór (5.5). Zauważmy, że dla $k = n = m$ wzór ten przyjmujc postać

(5.6) $$\binom{2n}{n} = \sum_{r=0}^{n} \binom{n}{r}^2.$$

Dla tożsamości

(5.7) $$\binom{n}{m}\binom{m}{k} = \binom{n}{k}\binom{n-k}{m-k}$$

łatwo znaleźć interpretację kombinatoryczną związaną ze zliczaniem na dwa sposoby par $\langle M, K\rangle$, gdzie $K \subseteq M \subseteq X$, $|K| = k$, $|M| = m$, $|X| = n$. Z jednej strony podzbiór M możemy wybrać na $\binom{n}{m}$ sposobów, a dla każdego takiego wyboru podzbiór $K \subseteq M$ na $\binom{m}{k}$ sposobów. Daje to $\binom{n}{m}\binom{m}{k}$ możliwych par (lewa strona (5.7)). Z drugiej strony podzbiór $K \subseteq X$ możemy wybrać na $\binom{n}{k}$ sposobów, a dla każdego takiego wyboru podzbiór M taki, że $K \subseteq M \subseteq X$ możemy wybrać na $\binom{n-k}{m-k}$ sposobów, tyle ile jest podzbiorów $(m-k)$-elementowych zbioru $X \setminus K$. Daje to $\binom{n}{k}\binom{n-k}{m-k}$ możliwych par (prawa strona (5.7)).

Udowodnimy teraz dwie tożsamości związane z sumami współczynników dwumiennych:

(5.8) $$\sum_{k=0}^{n} \binom{r+k}{k} = \binom{r+n+1}{n},$$

(5.9) $$\sum_{r=0}^{n} \binom{r}{k} = \binom{n+1}{k+1}.$$

Pierwsza z tych tożsamości jest związana ze zliczaniem na dwa sposoby n-elementowych podzbiorów $A \subseteq X = \{1, \ldots, r+n+1\}$. Podzbiory te możemy podzielić na grupy rozłączne ze względu na parametr $j = \min(X \setminus A)$. Łatwo zauważyć, że dla każdego j, $1 \leqslant j \leqslant n+1$, grupa taka zawiera $\binom{r+n+1-j}{n-(j-1)}$ $= \binom{r+(n-j+1)}{n-j+1}$ podzbiorów. Wystarczy teraz dokonać podstawienia $k = n-j+1$.

W podobny sposób (5.9) „zlicza" podzbiory $(k+1)$-elementowe zbioru $\{1, \ldots, n+1\}$ ze względu na parametr $r = n+1-j$, gdzie j jest elementem minimalnym podzbioru.

Inną pożyteczną tożsamością jest

(5.10) $$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}, \qquad n, k > 0.$$

Otrzymujemy ją łatwo, zliczając na dwa sposoby pary $\langle a, K\rangle$, gdzie $a \in K$, $K \subseteq X$, $|K| = k$, $|X| = n$. Z jednej strony, wybierając najpierw a, widzimy, że takich par jest $n\binom{n-1}{k-1}$. Z drugiej strony, wybierając najpierw K otrzymujemy wynik $\binom{n}{k}k$.

Wzór (5.10) zastosowany k-krotnie daje

$$(5.11)\qquad \binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k(k-1)\dots 1} = \frac{[n]_k}{k!} = \frac{n!}{k!(n-k)!}, \qquad 0 \leqslant k \leqslant n.$$

Równość $\binom{n}{k} = [n]_k/k!$ ma prostą interpretację kombinatoryczną. Wiemy, że $[n]_k$ jest liczbą ciągów różnowartościowych $\langle a_1, \dots, a_k\rangle$ o elementach ze zbioru n-elementowego. Każdy taki ciąg określa podzbiór k-elementowy $\{a_1, \dots, a_k\}$, przy czym ten sam podzbiór powstaje z dokładnie $k!$ ciągów odpowiadających jego wszystkim możliwym permutacjom.

Warto zauważyć, że każdy podzbiór zbioru $\{1, \dots, n\}$ można jednoznacznie reprezentować przez ciąg rosnący elementów tego podzbioru. Tak więc $\binom{n}{k}$ możemy również interpretować jako liczbę ciągów rosnących długości k o elementach ze zbioru $\{1, \dots, n\}$ (lub dowolnego innego zbioru n-elementowego liniowo uporządkowanego).

Dotychczas główną używaną przez nas metodą dowodu tożsamości związanych ze współczynnikami dwumiennymi było nadanie obu stronom pewnej interpretacji kombinatorycznej. Dla odmiany przedstawiamy teraz cztery różne metody dowodu na przykładzie tożsamości

$$(5.12)\qquad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \qquad n, k > 0.$$

Dowód I („rachunkowy"):

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} =$$
$$= \frac{n-k}{n}\,\frac{n!}{k!(n-k)!} + \frac{k}{n}\,\frac{n!}{k!(n-k)!} = \left(\frac{n-k}{n} + \frac{k}{n}\right)\binom{n}{k} = \binom{n}{k}.$$

Dowód II („algebraiczny"):

$$\sum_{k=0}^{n}\binom{n}{k}x^k = (1+x)^n = (1+x)(1+x)^{n-1} = (1+x)\sum_{k=0}^{n-1}\binom{n-1}{k}x^k =$$
$$= \sum_{k=0}^{n-1}\binom{n-1}{k}x^k + \sum_{k=0}^{n-1}\binom{n-1}{k}x^{k+1} =$$
$$= \sum_{k=0}^{n-1}\binom{n-1}{k}x^k + \sum_{k=1}^{n}\binom{n-1}{k-1}x^k.$$

Obie strony są wielomianami stopnia n, przy czym równość zachodzi dla dowolnego x. Stąd wniosek, że wielomiany te są tożsamościowo równe. Wystarczy teraz porównać współczynniki przy kolejnych potęgach x.

Dowód III („indukcyjny"): Stosujemy indukcję względem k i pomocniczo tożsamość (5.10). Dla $k = 1$ mamy $\binom{n}{1} = n = (n-1)+1 = \binom{n-1}{1}+\binom{n-1}{0}$, natomiast dla $k \geqslant 2$

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1} = \frac{1}{k}\left[\binom{n-1}{k-1}+(n-1)\binom{n-1}{k-1}\right] =$$

$$= \frac{1}{k}\left[\binom{n-1}{k-1}+(n-1)\binom{n-2}{k-1}+(n-1)\binom{n-2}{k-2}\right] =$$

$$= \frac{1}{k}\left[\binom{n-1}{k-1}+k\binom{n-1}{k}+(k-1)\binom{n-1}{k-1}\right] = \binom{n-1}{k}+\binom{n-1}{k-1}.$$

Dowód IV („kombinatoryczny"): Niech $|X| = n$, oraz $a \in X$. Zbiór wszystkich podzbiorów k-elementowych $K \subseteq X$ rozpada się na dwie rozłączne klasy, w zależności od tego czy $a \notin K$, czy też $a \in K$. Liczność pierwszej klasy wynosi oczywiście $\binom{n-1}{k}$, drugiej natomiast $\binom{n-1}{k-1}$.

Tożsamość (5.12) można zilustrować na następującym *trójkącie Pascala*:

$$\begin{array}{ccccccccc} & & & & 1 & & & & \\ & & & 1 & & 1 & & & \\ & & 1 & & 2 & & 1 & & \\ & 1 & & 3 & & 3 & & 1 & \\ 1 & & 4 & & 6 & & 4 & & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

Jeśli wiersze tego trójkąta ponumerujemy liczbami 0, 1, ..., to n-ty wiersz zawiera liczby $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$, przy czym równość $\binom{n}{k} = \binom{n-1}{k}+\binom{n-1}{k-1}$ dla $0 < k < n$ oznacza, że każdą liczbę w n-tym wierszu — z wyjątkiem skrajnych, równych jedności — można otrzymać jako sumę dwóch bezpośrednio nad nią występujących liczb w wierszu $n-1$. Fakt ten dostarcza prostego algorytmu obliczania współczynników dwumiennych. Wartości $\binom{n}{k}$ dla $0 \leqslant n, k \leqslant 10$, przedstawiono w tabl. 2.

Aby Czytelnik nie odniósł wrażenia, że każdą tożsamość dotyczącą współczynników dwumiennych można łatwo udowodnić nadając obu stronom interpretację kombinatoryczną, wykażemy teraz następującą tożsamość Li-Żen-Szua:

$$(5.13) \qquad \sum_{j=0}^{k}\binom{k}{j}^2\binom{n+2k-j}{2k} = \binom{n+k}{k}^2,$$

Tablica 2. Współczynniki dwumienne $\binom{n}{k}$

n \ k	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	1	1	0	0	0	0	0	0	0	0	0
2	1	2	1	0	0	0	0	0	0	0	0
3	1	3	3	1	0	0	0	0	0	0	0
4	1	4	6	4	1	0	0	0	0	0	0
5	1	5	10	10	5	1	0	0	0	0	0
6	1	6	15	20	15	6	1	0	0	0	0
7	1	7	21	35	35	21	7	1	0	0	0
8	1	8	28	56	70	56	28	8	1	0	0
9	1	9	36	84	126	126	84	36	9	1	0
10	1	10	45	120	210	252	210	120	45	10	1

dla której interpretacja kombinatoryczna jest dość skomplikowana (Surányi [1]; p. też Kaucký [1]). Poniższy dowód „rachunkowy" pochodzi od Huszára [1]. Najpierw mnożymy obie strony przez

$$\frac{(2k)!\,n!}{(n+k)!\,k!}.$$

Lewa strona przyjmuje postać

$$L = \sum_{j=0}^{k} \binom{k}{j} \frac{k!}{j!\,(k-j)!} \cdot \frac{(n+2k-j)!}{(2k)!\,(n-j)!} \cdot \frac{(2k)!\,n!}{(n+k)!\,k!} =$$

$$= \sum_{j=0}^{k} \binom{k}{j} \frac{n!}{j!\,(n-j)!} \cdot \frac{(n+2k-j)!}{(n+k)!\,(k-j)!} = \sum_{j=0}^{k} \binom{k}{j}\binom{n}{j}\binom{n+2k-j}{k-j},$$

natomiast po prawej stronie otrzymujemy

$$P = \binom{n+k}{k} \frac{(n+k)!}{k!\,n!} \cdot \frac{(2k)!\,n!}{(n+k)!\,k!} = \binom{n+k}{k}\binom{2k}{k}.$$

Korzystając z tożsamości Cauchy'ego (5.5) mamy:

$$L = \sum_{j=0}^{k} \binom{k}{j}\binom{n}{j} \sum_{r=0}^{k-j} \binom{n-j}{r}\binom{2k}{k-j-r},$$

albo, podstawiając $s = r+j$, czyli $r = s-j$,

$$L = \sum_{j=0}^{k} \binom{k}{j}\binom{n}{j} \sum_{s=j}^{k} \binom{n-j}{s-j}\binom{2k}{k-s} = \sum_{j=0}^{k} \binom{k}{j}\binom{n}{j} \sum_{s=0}^{k} \binom{n-j}{s-j}\binom{2k}{k-s},$$

i po zamianie porządku sumowania

$$L = \sum_{s=0}^{k} \binom{2k}{k-s} \sum_{j=0}^{s} \binom{k}{j}\binom{n}{j}\binom{n-j}{s-j}.$$

Stosując tożsamość Cauchy'ego do prawej strony mamy

$$P = \binom{2k}{k} \sum_{s=0}^{k} \binom{n}{s}\binom{k}{k-s}.$$

Zauważmy, że wystarczy teraz wykazać, że składniki (odpowiadające wskaźnikowi s) są równe po obu stronach, tzn. że

$$\binom{2k}{k-s} \sum_{j=0}^{s} \binom{k}{j}\binom{n}{j}\binom{n-j}{s-j} = \binom{2k}{k}\binom{n}{s}\binom{k}{k-s}.$$

Równość ta istotnie zachodzi, o czym można się przekonać stosując tożsamości (5.3), (5.5) i (5.7):

$$\binom{2k}{k-s} \sum_{j=0}^{s} \binom{k}{j}\binom{n}{j}\binom{n-j}{s-j} = \binom{2k}{k+s} \sum_{j=0}^{s} \binom{k}{j}\binom{n}{s}\binom{s}{j} = \binom{2k}{k+s}\binom{n}{s} \sum_{j=0}^{s} \binom{k}{j}\binom{s}{s-j} =$$

$$= \binom{n}{s}\binom{2k}{k+s}\binom{k+s}{s} = \binom{n}{s}\binom{2k}{k+s}\binom{k+s}{k} =$$

$$= \binom{n}{s}\binom{2k}{k}\binom{2k-k}{k+s-k} = \binom{n}{s}\binom{2k}{k}\binom{k}{s} = \binom{n}{s}\binom{2k}{k}\binom{k}{k-s}.$$

Dowód tożsamości Li-Żen-Szua jest tym samym zakończony.

Inne dowody tej tożsamości, jak również dowody wielu innych tożsamości związanych ze współczynnikami dwumiennymi, Czytelnik może znaleźć w monografii Kaucký'ego [1].

Symbol Newtona można łatwo uogólnić na przypadek, gdy górny wskaźnik jest dowolną liczbą rzeczywistą (lub zespoloną), korzystając ze wzoru $\binom{x}{k} = [x]_k/k!$ i traktując $[x]_k$ jako wielomian zmiennej x stopnia k, tak jak w poprzednim paragrafie. Tak więc $\binom{x}{k}$ jest wielomianem stopnia k, którego współczynniki wyrażają się, zgodnie ze wzorem (4.11), przez liczby Stirlinga pierwszego rodzaju:

(5.14) $$\binom{x}{k} = \sum_{j=0}^{k} \frac{s(k,j)}{k!} x^j.$$

Większość pokazanych przez nas tożsamości wielomianowych jest prawdziwa, gdy górne wskaźniki interpretujemy jako liczby rzeczywiste (idzie tu o zmienne nie związane operatorem sumowania, nie występujące jako ograniczenia dolne lub

górne wskaźników sumowania i nie występujące nigdzie jako część składowa dolnego wskaźnika w symbolu Newtona). Na przykład tożsamość (5.12) jest prawdziwa, gdy n jest dowolną liczbą rzeczywistą. Zauważmy jednak, że żaden z czterech przytoczonych przez nas dowodów nie obejmuje bezpośrednio tego ogólnego przypadku (dowód indukcyjny byłby dobry, gdybyśmy przedtem udowodnili tożsamość (5.10) dla przypadku n rzeczywistego; dowód rachunkowy można nieco zmodyfikować, tak by obejmował dowolną wartość n). Jednakże prawdziwość tożsamości (5.12) dla n rzeczywistego wynika z bardzo ogólnego faktu: po obu stronach mamy wielomiany zmiennej n, przy czym równość zachodzi dla nieskończenie wielu wartości n (dowolnego n naturalnego). A zatem wielomiany po obu stronach są równe tożsamościowo, gdyż wielomian będący ich różnicą, gdyby nie był tożsamościowo równy zeru, to miałby jedynie skończoną liczbę zer.

Na zakończenie tego paragrafu zajmiemy się pewnym uogólnieniem wzoru (5.1). Niech

$$(5.15)\qquad (x_1+\ldots+x_p)^n = \sum_{\substack{n_1,\ldots,n_p \geqslant 0\\ n_1+\ldots+n_p=n}} \binom{n}{n_1\, n_2 \ldots n_p} x_1^{n_1}\ldots x_p^{n_p},$$

przy czym równość tę traktujemy jako równość wielomianów definiującą współczynniki $\binom{n}{n_1\, n_2 \ldots n_p}$. Zauważmy, że $\binom{n}{n_1\, n_2 \ldots n_p}$ jest liczbą sposobów, na jakie w iloczynie $(x_1+\ldots+x_p)\ldots(x_1+\ldots+x_p)$ można wybrać x_1 w n_1 czynnikach, x_2 w n_2 czynnikach itd. (z każdego czynnika wybieramy dokładnie jeden składnik). Innymi słowy jest to liczba funkcji f: $\{1, \ldots, n\} \to \{1, \ldots, p\}$ takich, że $|f^{-1}(i)| = n_i$, $1 \leqslant i \leqslant p$. W terminach rozmieszczeń jest to liczba rozmieszczeń n elementów w p pudełkach takich, że i-te pudełko zawiera n_i elementów, dla $i = 1, \ldots, p$.

TWIERDZENIE 5.1. *Liczba funkcji* f: $\{1, \ldots, n\} \to \{1, \ldots, p\}$ *takich, że* $|f^{-1}(i)| = n_i$, $i = 1, \ldots, p$, *jest równa*

$$\binom{n}{n_1\, n_2 \ldots n_p} = \frac{n!}{n_1!\, n_2! \ldots n_p!}.$$

Dowód. Zbiór n_1 elementów, które przechodzą na element 1 przy odwzorowaniu f — tzn. zbiór elementów, które umieszczamy w pierwszym pudełku — możemy wybrać na $\binom{n}{n_1}$ sposobów. Spośród pozostałych $n-n_1$ elementów zbiór tych n_2 elementów, które umieszczamy w drugim pudełku możemy wybrać na $\binom{n-n_1}{n_2}$ sposobów itd. Powtarzając to rozumowanie

dochodzimy do wniosku, że poszukiwana liczba funkcji (rozmieszczeń) jest równa

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n_p}{n_p}=$$

$$=\frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\cdot\ldots\cdot\frac{n_p!}{n_p!}=$$

$$=\frac{n!}{n_1!n_2!\ldots n_p!}.\ \square$$

§ 6. Zbiory z powtórzeniami, podzielność liczb naturalnych

Niech X będzie dowolnym zbiorem i ustalmy w X dowolny porządek liniowy. Każdemu zbiorowi z powtórzeniami $(a_1, \ldots, a_k)$ o elementach z X możemy wtedy przyporządkować ciąg długości k zawierający elementy $a_1, \ldots, a_k$ uporządkowane niemalejąco względem naszego porządku liniowego. Łatwo zauważyć, że przyporządkowanie to ustala odpowiedniość wzajemnie jednoznaczną między k-elementowymi zbiorami z powtórzeniami o elementach z X a ciągami niemalejącymi długości k o elementach z X. Jest to oczywiście rozszerzenie rozważanej w poprzednim paragrafie odpowiedniości między zbiorami bez powtórzeń a ciągami rosnącymi.

Obliczymy teraz liczbę k-elementowych zbiorów z powtórzeniami o elementach ze zbioru n-elementowego X (są one tradycyjnie nazywane w starszej literaturze *kombinacjami k-wyrazowymi ze zbioru n-elementowego z powtórzeniami*). Bez zmniejszenia ogólności możemy zakładać, że $X = \{1, \ldots, n\}$. Zauważmy teraz, że przyporządkowując ciągowi $\langle a_1, \ldots, a_k\rangle$ ciąg $\langle a_1, a_2+1, \ldots, a_k+(k-1)\rangle$ ustalamy odpowiedniość wzajemnie jednoznaczną między ciągami niemalejącymi o elementach ze zbioru $\{1, \ldots, n\}$ a ciągami rosnącymi o elementach ze zbioru $\{1, \ldots, n+k-1\}$. Istotnie, warunek $a_i \leqslant a_{i+1}$ jest równoważny warunkowi $a_i+(i-1) < a_{i+1}+i$. Na mocy naszych poprzednich uwag i twierdzenia 5.1 otrzymujemy następujące twierdzenie:

TWIERDZENIE 6.1. *Liczba k-elementowych zbiorów z powtórzeniami o elementach ze zbioru n-elementowego jest równa*

$$\binom{n+k-1}{k}.\ \square$$

Odnotujemy jeszcze inne sformułowanie tego samego faktu:

TWIERDZENIE 6.2. *Istnieje dokładnie* $\binom{n+k-1}{k}$ *funkcji niemalejących* $f\colon \{1, \ldots, k\} \to \{1, \ldots, n\}$. $\square$

Zauważmy, że współczynnik dwumienny $\binom{n+k-1}{k}$ można zapisać jako

(6.1) $$\binom{n+k-1}{k} = \frac{[n]^k}{k!}.$$

Fakt ten ma prostą interpretację kombinatoryczną. Rozważmy wszystkie rozmieszczenia uporządkowane k elementów w n pudełkach. Niech $x_1, \ldots, x_n$ będą dowolnymi elementami ($x_i \neq x_j$ dla $i \neq j$). Przyporządkujmy dowolnemu rozmieszczeniu zawierającemu r_i elementów w i-tym pudełku ($i = 1, \ldots, n$; $r_1 + \ldots + r_n = k$) k-elementowy zbiór z powtórzeniami $(r_1 * x_1, \ldots, r_n * x_n)$. Zauważmy, że w przyporządkowaniu tym istotna jest jedynie liczba elementów znajdujących się w każdym pudełku, nieistotne jest natomiast jakie to są elementy. Tak więc otrzymamy ten sam zbiór z powtórzeniami, jeśli dokonamy dowolnej permutacji elementów na zajmowanych przez nie k pozycjach w naszym rozmieszczeniu. Wszystkich rozmieszczeń uporządkowanych jest $[n]^k$ (p. twierdzenie 3.4), liczba podzbiorów k-elementowych zbioru $(k * x_1, \ldots, k * x_n)$ jest więc równa $[n]^k/k!$. Oczywiście rozumowanie to, wraz z równością (6.1), stanowi niezależny dowód twierdzenia 6.1.

Oznaczmy przez $\mathcal{M}(X)$ rodzinę wszystkich zbiorów skończonych z powtórzeniami o elementach ze zbioru (niekoniecznie skończonego) X. Wtedy twierdzenie 6.1 określa liczbę elementów rangi k zbioru częściowo uporządkowanego $\langle \mathcal{M}(X), \subseteq \rangle$ (przypomnijmy, że $A \subseteq B$ wtedy i tylko wtedy, gdy $r_A(x) \leqslant r_B(x)$ dla każdego $x \in X$). Zauważmy, że skoro każdy zbiór z powtórzeniami $A \in \mathcal{M}(X)$ możemy utożsamiać z funkcją $r_A\colon X \to N_0$, która przyjmuje wartości różne od zera jedynie dla skończonej liczby argumentów, to zbiór $\langle \mathcal{M}(X), \subseteq \rangle$ jest izomorficzny z sumą prostą $\bigoplus_{x \in X} P_x$, gdzie P_x jest łańcuchem $\langle N_0, \leqslant \rangle$ dla każdego $x \in X$. Szczególnie ważny jest przypadek, gdy X jest zbiorem przeliczalnym, np. $X = N$.

TWIERDZENIE 6.3. $\langle \mathcal{M}(N), \subseteq \rangle \simeq \langle N, | \rangle$.

Dowód. Niech $p_1, p_2, \ldots$ będą kolejnymi liczbami pierwszymi. Na mocy fundamentalnego twierdzenia o rozkładzie na czynniki pierwsze każdą liczbę naturalną n można przedstawić jednoznacznie w postaci $n = \prod_{j=1}^{\infty} p_j^{\alpha_j}$, gdzie $\alpha_j(n) \neq 0$ tylko dla skończonej liczby wskaźników j. Określmy odwzorowanie $f\colon \mathcal{M}(N) \to N$ następująco:

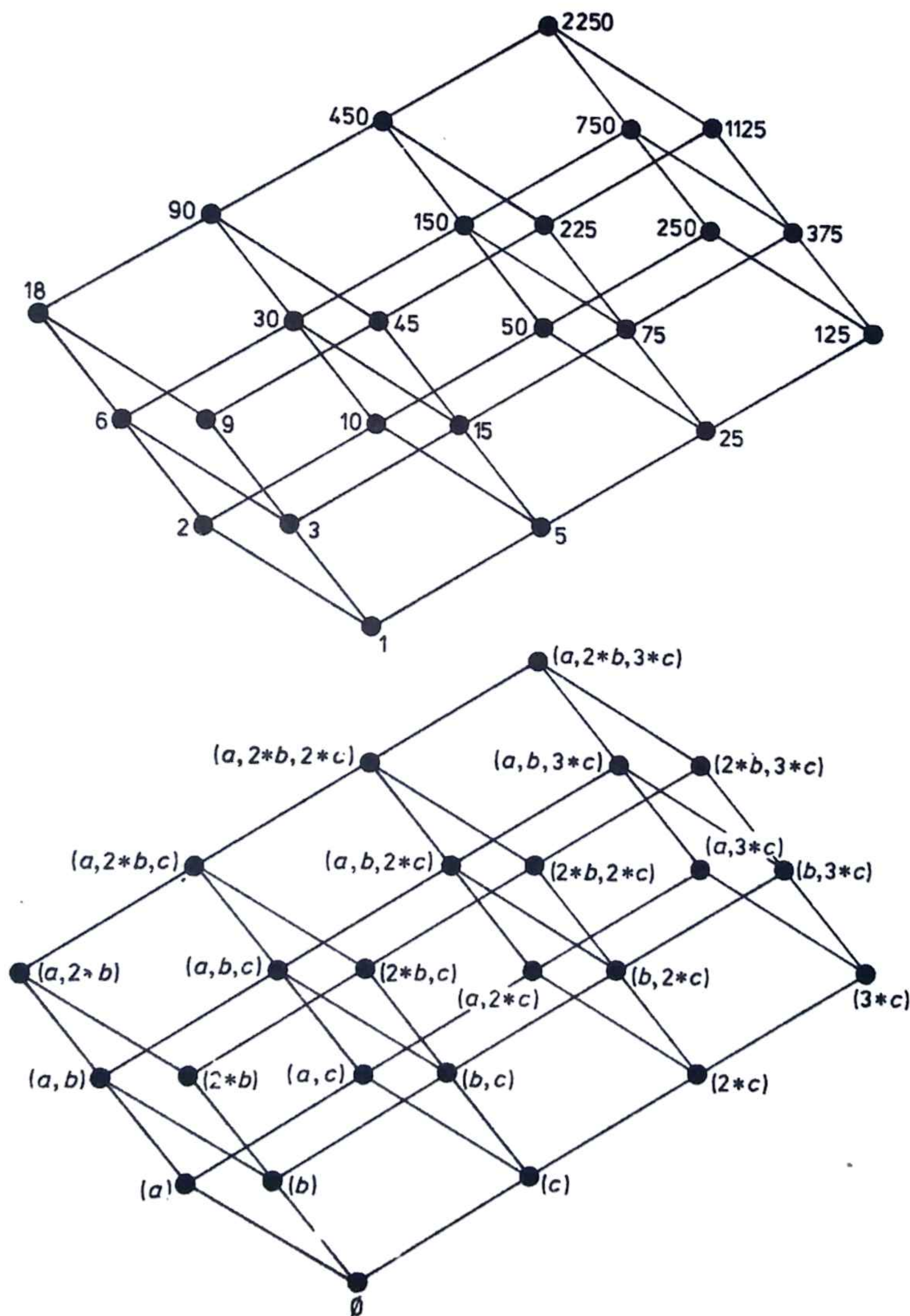
$$f(A) = \prod_{j=1}^{\infty} p_j^{r_A(j)}.$$

Z jednoznaczności rozkładu na czynniki pierwsze wynika, że f jest odwzorowaniem wzajemnie jednoznacznym $\mathcal{M}(N)$ na N. Co więcej, dla dowolnych

$A, B \in \mathcal{M}(N)$

$$A \subseteq B \Leftrightarrow f(A) | f(B),$$

jako że $n|m$ wtedy i tylko wtedy, gdy wykładnik w potędze każdej liczby pierwszej w rozkładzie liczby n na czynniki pierwsze jest niewiększy od analogicznego wykładnika w rozkładzie liczby m. Funkcja f określa zatem izomorfizm zbiorów częściowo uporządkowanych $\langle \mathcal{M}(N), \subseteq \rangle$ i $\langle N, | \rangle$. □



Rys. 6. Izomorfizm pomiędzy odcinkiem [1, 2250] porządku $\langle N, | \rangle$ a porządkiem $\langle \mathcal{P}(A), \subseteq \rangle$, gdzie $A = (a, 2*b, 3*c)$

Na rys. 6 przedstawiono odcinek [1, 2250] porządku $\langle \boldsymbol{N}, | \rangle$ oraz izomorficzny z nim porządek $\langle \mathscr{P}(A), \subseteq \rangle$, gdzie $A = (a, 2*b, 3*c)$ $(2250 = 2 \cdot 3^2 \cdot 5^3)$. Rysunek ten ilustruje też fakt — oczywisty wobec powyższych rozważań — że ogólnie, krata podzbiorów zbioru $(r_1 * a_1, \ldots, r_k * a_k)$, a więc i izomorficzna z nią krata podzielników liczby $p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$, jest izomorficzna z iloczynem kartezjańskim $C_{r_1} \times \ldots \times C_{r_k}$, gdzie C_{r_i} jest łańcuchem długości r_i (tzn. składającym się z $r_i + 1$ elementów). Zauważmy, że w kracie podzbiorów działania kratowe są zwykłymi działaniami sumy i przecięcia zbiorów z powtórzeniami,

$$A \vee B = A \cup B, \qquad A \wedge B = A \cap B,$$

w kracie podzielników natomiast odpowiednie działania, to

$$a \vee b = [a, b] \quad \text{(najmniejsza wspólna wielokrotność)},$$
$$a \wedge b = (a, b) \quad \text{(największy wspólny podzielnik)}.$$

§ 7. Zasada włączania–wyłączania

Typowy problem, którym będziemy się zajmowali w tym paragrafie, można sformułować następująco: Dany jest ciąg $P_1, \ldots, P_k$ podzbiorów zbioru skończonego X (a więc k własności elementów zbioru X, jako że własność możemy identyfikować ze zbiorem elementów, które ją mają). Nie zakładamy przy tym, że zbiory te są różne. Dla dowolnego $r \leqslant k$ i dla dowolnego ciągu $1 \leqslant i_1 < \ldots < i_r \leqslant k$ oznaczmy

(7.1) $$N(i_1, \ldots, i_r) = |P_{i_1} \cap \ldots \cap P_{i_r}|$$

oraz

(7.2) $$W(r) = \sum N(i_1, \ldots, i_r),$$

gdzie sumowanie rozciąga się po wszystkich ciągach postaci $1 \leqslant i_1 < \ldots < i_r \leqslant k$ (przyjmujemy $W(0) = |X|$). Niech wreszcie $D(r)$ oznacza liczność zbioru tych $x \in X$, które należą do dokładnie r spośród zbiorów $P_1, \ldots, P_k$. Naszym zadaniem będzie wyznaczenie wartości $D(r)$ na podstawie wartości $W(s)$, $1 \leqslant s \leqslant k$.

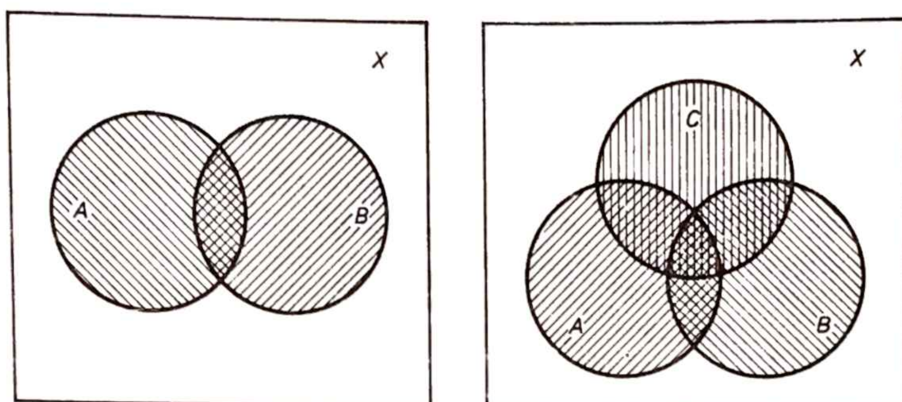
Zanim podamy ogólny wzór, rozważmy kilka prostych przypadków szczególnych. Niech $r = 0$, $k = 2$. Wtedy

$$D(0) = |X| - |P_1 \cup P_2| = |X| - |P_1| - |P_2| + |P_1 \cap P_2| =$$
$$= W(0) - W(1) + W(2).$$

Podobnie dla $r = 0$, $k = 3$ otrzymujemy

$$D(0) = |X| - |P_1 \cup P_2 \cup P_3| =$$
$$= |X| - |P_1| - |P_2| - |P_3| + |P_1 \cap P_2| + |P_2 \cap P_3| + |P_1 \cap P_3| - |P_1 \cap P_2 \cap P_3| =$$
$$= W(0) - W(1) + W(2) - W(3).$$

Wzory te zilustrowano na rys. 7.



Rys. 7. Proste przypadki zasady włączania–wyłączania

$$|A \cup B| = |X| - W(0) = W(1) - W(2) = |A| + |B| - |A \cap C|$$

$$|A \cup B \cup C| = |X| - W(0) = W(1) - W(2) + W(3) =$$
$$= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

Podamy teraz wzór ogólny dla dowolnego k i r.

TWIERDZENIE 7.1. *Dla dowolnych* $k > 0$ *oraz* $r \leqslant k$

$$D(r) = \sum_{j=0}^{k-r} (-1)^j \binom{r+j}{r} W(r+j).$$

Dowód. Zauważmy najpierw, że lewą i prawą stronę naszej równości możemy zapisać odpowiednio jako $\sum_{x \in X} L(x)$ oraz $\sum_{x \in X} R(x)$, gdzie wkład $L(x)$ wnoszony przez element x do lewej strony jest równy

$$L(x) = \begin{cases} 1, & \text{jeśli } x \text{ należy do dokładnie } r \text{ spośród zbiorów } P_1, \ldots, P_k, \\ 0, & \text{w przeciwnym przypadku,} \end{cases}$$

i podobnie, udział $R(x)$ elementu x w prawej stronie wyraża się wzorem

(7.3) $$R(x) = \sum_{j=0}^{k-r} (-1)^j \binom{r+j}{r} R_{r+j}(x),$$

gdzie $R_{r+j}(x)$ jest liczbą ciągów postaci $1 \leqslant i_1 < \ldots < i_{r+j} \leqslant k$ takich, że $x \in P_{i_1} \cap \ldots \cap P_{i_{r+j}}$. Wykażemy, że dla każdego $x \in X$ mamy $L(x) = R(x)$, co zakończy dowód.

Niech $x \in X$ i załóżmy, że x należy do dokładnie u spośród zbiorów $P_1, \ldots, P_k$. Możliwe są trzy przypadki:

$u < r$. Wtedy oczywiście $L(x) = 0$. Podobnie $R(x) = 0$, dla każdego bowiem $m \geqslant r$ i każdego ciągu $1 \leqslant i_1 < \ldots < i_m \leqslant k$ mamy $x \notin P_{i_1} \cap \ldots \cap P_{i_k}$ i w konsekwencji $R_m(x) = 0$.

$u = r$. Mamy wtedy $L(x) = 1$ i podobnie $R(x) = 1$, jako że $R_{r+j}(x) = 0$ dla $j > 0$ oraz $(-1)^0 \binom{r+0}{r} R_{r+0}(x) = R_r(x) = 1$.

$u > r$. Wtedy oczywiście $L(x) = 0$. Zauważmy, że $R_m(x) = \binom{u}{m}$, jako że na tyle właśnie sposobów możemy spośród u wskaźników zbiorów zawierających element x utworzyć ciąg rosnący długości m. Podstawiając tę wartość do wzoru (7.3), korzystając następnie z tożsamości (5.7), (5.3) i wreszcie z tożsamości (5.4) otrzymujemy:

$$R(x) = \sum_{j=0}^{k-r} (-1)^j \binom{r+j}{r}\binom{u}{r+j} = \sum_{j=0}^{u-r} (-1)^j \binom{r+j}{r}\binom{u}{r+j} =$$

$$= \sum_{j=0}^{u-r} (-1)^j \binom{u}{r}\binom{u-r}{u-r-j} = \binom{u}{r} \sum_{j=0}^{u-r} (-1)^j \binom{u-r}{j} = 0.$$

Dowód jest tym samym zakończony. □

W zastosowaniach ważny jest przypadek $r = 0$. Wtedy $\binom{r+j}{r} = 1$ i twierdzenie 7.1 przyjmuje następującą postać:

WNIOSEK 7.2 (*Zasada włączania–wyłączania*)

$$D(0) = \sum_{j=0}^{k} (-1)^j W(j). \quad \square$$

Wzór ten jest też czasem nazywany *formułą sita*.

W rozdziale 2 znajdzie Czytelnik inny dowód twierdzenia 7.1 oraz innych wzorów tego typu, jak również wiele zastosowań tych twierdzeń. W tym miejscu podamy jedynie kilka najprostszych zastosowań.

TWIERDZENIE 7.3. *Jeśli $|X| = n$, $|Y| = m$, to liczba s_{nm} wszystkich funkcji z X na Y jest równa*

$$s_{nm} = \sum_{j=0}^{m} (-1)^j \binom{m}{j} (m-j)^n.$$

Dowód. Niech $Y = \{y_1, \ldots, y_m\}$ i niech P_i będzie zbiorem funkcji $f\colon X \to Y$, dla których $y_i \notin f(X)$. Funkcja $f\colon X \to Y$ jest odwzorowaniem na cały zbiór Y wtedy i tylko wtedy, gdy nie należy do żadnego ze zbiorów P_i, $1 \leqslant i \leqslant m$. Liczba funkcji z X na Y jest więc — przy oznaczeniach wprowadzonych w tym paragrafie — równa $D(0)$. Aby skorzystać z zasady włączania–wyłączania wystarczy zatem wyznaczyć liczność przecięcia $P_{k_1} \cap \ldots \cap P_{k_j}$ dla dowolnego ciągu $1 \leqslant k_1 < \ldots < k_j \leqslant m$. Łatwo zauważyć, że przecięcie to jest zbiorem wszystkich funkcji $f\colon X \to Y \setminus \{y_{k_1}, \ldots, y_{k_j}\}$, jego liczność wynosi więc $(m-j)^n$, tyle, ile jest

wszystkich funkcji ze zbioru n-elementowego w zbiór $(m-j)$-elementowy (por. twierdzenie 3.1). Ciąg $1 \leqslant k_1 < \ldots < k_j \leqslant m$ możemy wybrać na $\binom{m}{j}$ sposobów, co daje $W(j) = \binom{m}{j}(m-j)^n$ i ostatecznie

$$s_{nm} = D(0) = \sum_{j=0}^{m} (-1)^j W(j) = \sum_{j=0}^{m} (-1)^j \binom{m}{j}(m-j)^n. \quad \square$$

Na zakończenie tego paragrafu wyznaczymy jeszcze liczbę tzw. nieporządków. *Nieporządkiem* na zbiorze X nazywamy dowolną permutację $f\colon X \to X$ taką, że $f(x) \neq x$ dla każdego $x \in X$. Oznaczmy przez D_n liczbę nieporządków na zbiorze n-elementowym.

TWIERDZENIE 7.4.

$$D_n = \sum_{j=0}^{n} (-1)^j \binom{n}{j}(n-j)!.$$

Dowód. Bez zmniejszenia ogólności możemy przyjąć $X = \{1, \ldots, n\}$. Oznaczmy przez P_i zbiór tych permutacji $f\colon X \to X$, dla których $f(i) = i$. Liczność zbioru wszystkich nieporządków, to wtedy nic innego jak $D(0)$. Dla dowolnego ciągu $1 \leqslant k_1 < \ldots < k_j \leqslant n$ przecięcie $P_{k_1} \cap \ldots \cap P_{k_j}$ jest oczywiście zbiorem wszystkich tych permutacji f, dla których $f(k_s) = k_s$, $s = 1, \ldots, j$. Takich permutacji jest $(n-j)!$, tyle, ile wszystkich permutacji zbioru $X \setminus \{k_1, \ldots, k_j\}$. Biorąc pod uwagę fakt, iż ciąg $1 \leqslant k_1 < \ldots < k_j \leqslant n$ możemy wybrać na $\binom{n}{j}$ sposobów i korzystając z zasady włączania–wyłączania otrzymujemy ostatecznie

$$D_n = \sum_{j=0}^{n} (-1)^j W(j) = \sum_{j=0}^{n} (-1)^j \binom{n}{j}(n-j)!. \quad \square$$

Zauważmy, że powyższy wzór możemy zapisać nieco inaczej:

$$D_n = \sum_{j=0}^{n} (-1)^j \binom{n}{n-j}(n-j)! = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}.$$

To znaczy, że przy $n \to \infty$ nieporządki stanowią asymptotycznie $\sum_{i=0}^{\infty} (-1)^i/i! = e^{-1} = 0.36788\ldots$ wszystkich permutacji.

§ 8. Podziały zbioru, liczby Stirlinga drugiego rodzaju

Przypomnijmy, że przez podział zbioru X na k bloków rozumiemy dowolną rodzinę $\pi = \{B_1, \ldots, B_k\}$ taką, że $X = B_1 \dot{\cup} \ldots \dot{\cup} B_k$ oraz $B_i \neq \emptyset$ dla $1 \leqslant i \leqslant k$. Zbiór wszystkich podziałów zbioru X na k bloków będziemy oznaczali przez

$\Pi_k(X)$, zbiór zaś wszystkich podziałów zbioru X przez $\Pi(X)$. Jeśli $|X| = n$, to

$$\Pi(X) = \Pi_1(X) \dot{\cup} \ldots \dot{\cup} \Pi_n(X),$$

co więcej, $\{\Pi_1(X), \ldots, \Pi_n(X)\}$ jest podziałem zbioru $\Pi(X)$, gdyż zbiór $\Pi_i(X)$ jest oczywiście niepusty dla $i = 1, \ldots, n$.

Jak już wspomniano w paragrafie 1, istnieje odpowiedniość wzajemnie jednoznaczna pomiędzy podziałami zbioru X a relacjami równoważności na zbiorze X, przy której podziałowi π odpowiada relacja równoważności

$$E(\pi) = \bigcup_{B \in \pi} (B \times B),$$

relacji równoważności R natomiast odpowiada podział $P(R)$ zbioru X na klasy abstrakcji tej relacji:

$$P(R) = \{[x]_R \colon x \in X\}.$$

Niech $\pi, \sigma \in \Pi(X)$. Będziemy mówili, że podział π jest *rozdrobnieniem* podziału σ, co będziemy oznaczali przez $\pi \leqslant \sigma$, jeśli każdy blok $B \in \sigma$ jest sumą pewnej liczby bloków podziału π. Na przykład

$$\{\{1\}, \{2, 4\}, \{3, 5\}, \{6\}, \{7\}\} \leqslant \{\{1, 6\}, \{2, 3, 4, 5\}, \{7\}\}.$$

Oczywiście $\pi \leqslant \sigma$ jest równoważne temu, by każdy blok $B \in \pi$ był zawarty w pewnym bloku podziału σ. Łatwo zauważyć, że ten ostatni warunek jest z kolei równoważny warunkowi $E(\pi) \subseteq E(\sigma)$.

Relacja $\leqslant$ jest oczywiście porządkiem częściowym na zbiorze $\Pi(X)$ (p. rys. 8). Co więcej, zachodzi następujące twierdzenie:

TWIERDZENIE 8.1. *Zbiór częściowo uporządkowany* $\langle \Pi(X), \leqslant \rangle$ *jest kratą, przy czym*

(8.1) $$\pi \wedge \sigma = \{A \cap B \colon (A \in \pi) \wedge (B \in \sigma) \wedge (A \cap B \neq \emptyset)\},$$

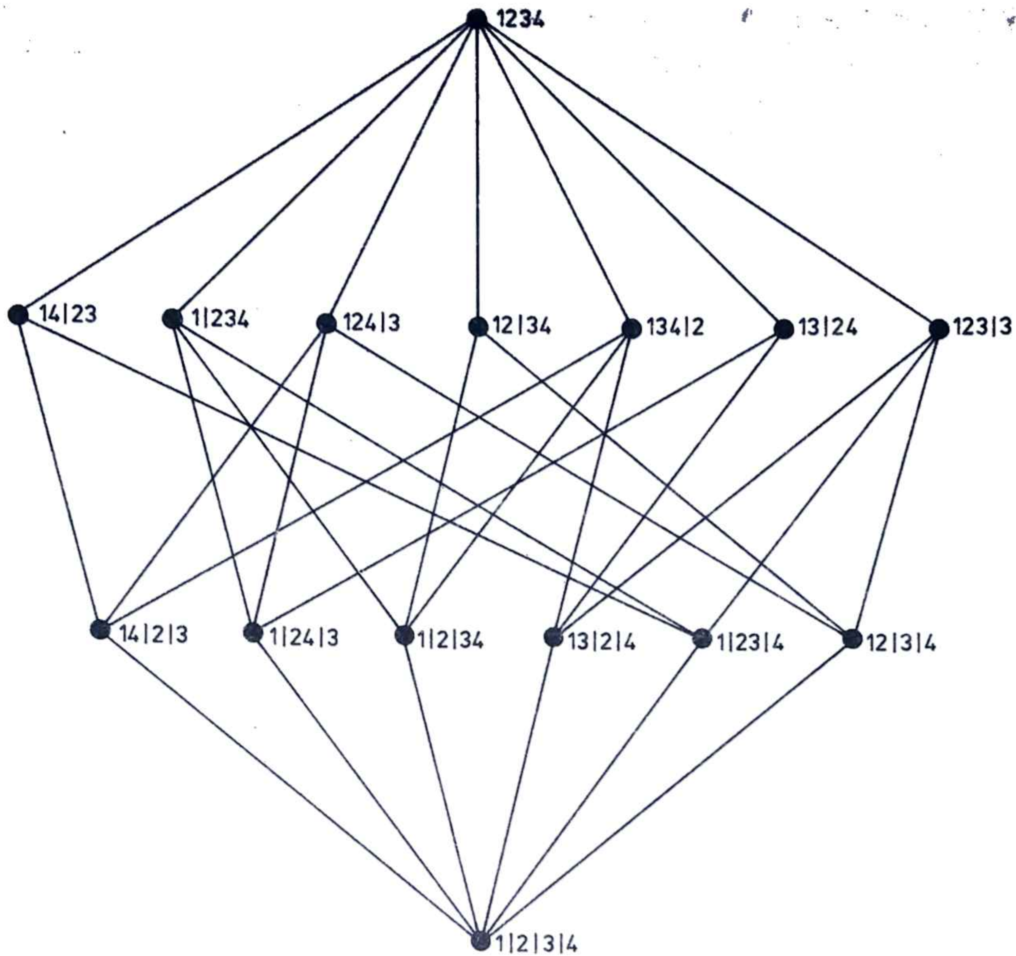
tzn.

$$E(\pi \wedge \sigma) = E(\pi) \cap E(\sigma),$$

podział $\pi \vee \sigma$ *jest natomiast określony następująco:*

(8.2) $\langle x, y \rangle \in E(\pi \vee \sigma) \Leftrightarrow$ *istnieje* $k \geqslant 1$ *oraz ciąg* $x_1, \ldots, x_k$ *taki, że* $x = x_1$, $y = y_k$ *oraz* $\langle x_i, x_{i+1} \rangle \in E(\pi)$ *lub* $\langle x_i, x_{i+1} \rangle \in E(\sigma)$ *dla* $i = 1, \ldots, k-1$.

Dowód. Zauważmy przede wszystkim, że bezpośrednio z definicji relacji równoważności wynika fakt, iż przecięcie dowolnej rodziny relacji równoważności na X jest relacją równoważności na X (jako przecięcie rodziny pustej przyjmujemy relację równoważności $X \times X$). Wynika stąd, że zbiór $\mathscr{R}(X)$ wszystkich relacji równoważności na X uporządkowany przez inkluzję tworzy kratę. Istotnie, dla



Rys. 8. Częściowy porządek $\langle \Pi(X), \leqslant \rangle$, $X = \{1, 2, 3, 4\}$ (podziały są oznaczone w uproszczony sposób, np. 14|2|3 oznacza $\{\{1, 4\}, \{2\}, \{3\}\}$)

dowolnych $R, S \in \mathscr{R}(X)$ mamy

$$R \wedge S = R \cap S,$$

$$R \vee S = \bigcap \{T \in \mathscr{R}(X)\colon (R \subseteq T) \wedge (S \subseteq T)\}.$$

Zbiór $\langle \Pi(X), \leqslant \rangle$, izomorficzny na mocy naszych poprzednich rozważań z $\langle \mathscr{R}(X), \subseteq \rangle$, jest więc również kratą.

Należy jeszcze wykazać, że działania w tej kracie określone są istotnie wzorami (8.1) i (8.2). W przypadku pierwszego wzoru wystarczy zauważyć, że $\langle x, y \rangle \in E(\pi) \cap E(\sigma)$ wtedy i tylko wtedy, gdy x i y należą do pewnego bloku $A \in \pi$ i pewnego bloku $B \in \sigma$, tzn. $x, y \in A \cap B$.

Aby udowodnić wzór (8.2), załóżmy, że R jest relacją binarną złożoną z tych par $\langle x, y \rangle \in X \times X$, które spełniają prawą stronę tego wzoru. Łatwo sprawdzić, że jest to relacja równoważności: $x R x$ (wystarczy przyjąć $k = 1$), $x R y$ pociąga za sobą $y R x$ (wystarczy rozważyć ciąg $x_k, x_{k-1}, \ldots, x_1$) oraz $x R y$, $y R z$ pociąga za sobą $x R z$ (wystarczy rozważyć konkatenację odpowiednich ciągów). Niech β będzie podziałem odpowiadającym relacji R, tzn. $E(\beta) = R$. Oczywiście $E(\pi) \subseteq R$

$= E(\beta)$ i $E(\sigma) \subseteq R = E(\beta)$, a więc $\pi \leqslant \beta$ i $\sigma \leqslant \beta$. Rozważmy dowolny podział β' taki, że $\pi \leqslant \beta'$, $\sigma \leqslant \beta'$, i niech $\langle x, y\rangle \in E(\beta)$. Istnieje wtedy ciąg $x_1, \ldots, x_k$ spełniający prawą stronę równoważności (8.2), i w konsekwencji $\langle x_i, x_{i+1}\rangle \in E(\pi) \cup E(\sigma) \subseteq E(\beta')$, $1 \leqslant i \leqslant k$. Wobec przechodniości relacji $R(\beta')$ mamy $\langle x_1, x_k\rangle = \langle x, y\rangle \in E(\beta')$. Wykazaliśmy więc, że $E(\beta) \subseteq E(\beta')$, tzn. $\beta \leqslant \beta'$, co oznacza, iż β jest istotnie najmniejszym ograniczeniem górnym elementów π, σ zbioru częściowo uporządkowanego $\langle \Pi(X), \leqslant\rangle$. □

Będziemy mówili, że podział π zbioru n-elementowego X jest *typu* $\lambda = \langle \lambda_1, \ldots, \lambda_n\rangle$, jeśli zawiera on dokładnie λ_i bloków liczności i. Zauważmy tu związek z rozważanym w paragrafie 4 pojęciem typu permutacji: permutacja zbioru X jest typu λ wtedy i tylko wtedy, gdy podział zbioru X określony przez rozkład tej permutacji na cykle jest typu λ. Podobnie jak w przypadku permutacji typ $\langle \lambda_1, \ldots, \lambda_n\rangle$ podziału będziemy zapisywali symbolicznie jako $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$. Oczywiście typ dowolnego podziału zbioru n-elementowego spełnia zależność

$$\sum_{i=1}^{n} i\lambda_i = n.$$

TWIERDZENIE 8.2. *Liczba podziałów typu* $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ *zbioru n-elementowego* $(\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n = n)$ *jest równa*

$$P(\lambda_1, \ldots, \lambda_n) = \frac{n!}{\lambda_1!\lambda_2!\ldots\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\ldots(n!)^{\lambda_n}}.$$

Dowód. Skorzystamy ze wzoru na liczbę $h(\lambda_1, \ldots, \lambda_n)$ permutacji typu $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ (por. twierdzenie 4.2).

Jak już zauważyliśmy, każdej permutacji typu $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ odpowiada podział tego samego typu określony przez rozkład permutacji na cykle. Ten sam podział powstaje z dokładnie $(1!)^{\lambda_2}(2!)^{\lambda_3}\ldots((n-1)!)^{\lambda_n}$ permutacji, gdyż każdy blok liczności i możemy zorientować cyklicznie na $(i-1)!$ sposobów. Stąd

$$P(\lambda_1, \ldots, \lambda_n) = \frac{h(\lambda_1, \ldots, \lambda_n)}{(1!)^{\lambda_2}(2!)^{\lambda_3}\ldots((n-1)!)^{\lambda_n}} =$$

$$= \frac{n!}{1^{\lambda_1} 2^{\lambda_2}\ldots n^{\lambda_n}\lambda_1!\lambda_2!\ldots\lambda_n!(1!)^{\lambda_2}(2!)^{\lambda_3}\ldots((n-1)!)^{\lambda_n}} =$$

$$= \frac{n!}{\lambda_1!\lambda_2!\ldots\lambda_n!(1!)^{\lambda_1}(2!)^{\lambda_2}\ldots(n!)^{\lambda_n}}. \; \square$$

Liczbę podziałów zbioru n-elementowego na k bloków oznaczamy przez $S(n, k)$ i nazywamy *liczbą Stirlinga drugiego rodzaju*. Tak więc

$$S(n, k) = |\Pi_k(X)|, \quad \text{gdzie } |X| = n.$$

Jeszcze inaczej możemy powiedzieć, że $S(n, k)$ jest liczbą elementów rangi $n-k$ w zbiorze częściowo uporządkowanym $\langle \Pi(X), \leqslant \rangle$, gdzie $|X| = n$, np. $X = \{1, \ldots, n\}$. Istotnie, zerem w tym zbiorze – a więc jedynym elementem rangi zero – jest podział najdrobniejszy $\{\{1\}, \ldots, \{n\}\} \in \Pi_n(X)$. Jeśli $\pi \in \Pi_k(X)$ oraz σ jest bezpośrednim następnikiem podziału π względem porządku $\leqslant$, to łatwo zauważyć, że σ powstaje z π przez zastąpienie pewnych dwóch bloków podziału π ich sumą, a więc $\sigma \in \Pi_{k-1}(X)$. Stąd już łatwo wynika, że $\Pi_k(X)$ jest dokładnie zbiorem elementów rangi $n-k$ w $\langle \Pi(X), \leqslant \rangle$.

Z twierdzenia 8.2 wynika następujący wzór na liczby Stirlinga drugiego rodzaju:

$$S(n, k) = \sum \frac{n!}{\lambda_1! \lambda_2! \ldots \lambda_n! (1!)^{\lambda_1} (2!)^{\lambda_2} \ldots (n!)^{\lambda_n}},$$

gdzie sumowanie rozciąga się na wszystkie ciągi $\langle \lambda_1, \ldots, \lambda_n \rangle$ takie, że $\lambda_1 + \lambda_2 + \ldots + \lambda_n = k$ oraz $\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n = n$. W dalszym ciągu pokażemy znacznie prostszy wzór.

Istnieje ścisły związek liczb Stirlinga drugiego rodzaju z rozważaną w poprzednim paragrafie liczbą s_{nk} wszystkich funkcji ze zbioru n-elementowego na zbiór k-elementowy. Każdej funkcji $f\colon X \to Y$, gdzie $f(X) = Y$, możemy przyporządkować podział zbioru X na k bloków

$$N(f) = \{f^{-1}(y)\colon y \in Y\},$$

zwany *jądrem* funkcji f (warunek $f(X) = Y$ gwarantuje, że podzbiory $f^{-1}(y)$ są niepuste). Jądro funkcji określa dokładnie, które elementy zbioru X przechodzą na te same elementy zbioru Y, nie wyznacza jednak konkretnie tych elementów. Łatwo zauważyć, że dla każdego podziału $\pi \in \Pi_k(X)$ istnieje dokładnie $k!$ funkcji z X na Y takich, że $N(f) = \pi$. Każda taka funkcja odpowiada pewnemu spośród $k!$ wzajemnie jednoznacznych przyporządkowań elementów zbioru Y blokom podziału π. Otrzymujemy stąd następującą prostą zależność:

(8.3) $$s_{nk} = k!\, S(n, k).$$

Korzystając z twierdzenia 7.3 mamy więc

(8.4) $$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} (-1)^j \binom{k}{j} (k-j)^n.$$

Wygodniejszym od użycia powyższego wzoru sposobem wyznaczania liczb Stirlinga drugiego rodzaju jest skorzystanie z zależności rekurencyjnych będących treścią następnego twierdzenia.

TWIERDZENIE 8.3. *Liczby Stirlinga drugiego rodzaju spełniają zależności*

(8.5) $S(n, n) = 1$ *dla* $n \geqslant 0$,

(8.6) $S(n, 0) = 0$ *dla* $n > 0$,

(8.7) $S(n, k) = S(n-1, k-1) + kS(n-1, k)$ *dla* $0 < k < n$.

Dowód. Pierwsze dwa wzory są oczywiste. (Zauważmy, że $S(0, 0) = 1$, gdyż pusta rodzina bloków jest – zgodnie z definicją – jedynym podziałem zbioru pustego na zerową liczbę bloków). Dla dowodu zależności (8.7) rozważmy zbiór wszystkich podziałów zbioru $\{1, \ldots, m\}$ na k bloków. Zbiór ten rozpada się na dwie rozłączne klasy: tych podziałów, które zawierają blok postaci $\{n\}$, oraz tych, dla których element n występuje w bloku co najmniej dwuelementowym. Liczność pierwszej klasy wynosi oczywiście $S(n-1, k-1)$, tyle, ile jest podziałów zbioru $\{1, \ldots, n-1\}$ na $k-1$ bloków. Liczność drugiej klasy wynosi $kS(n-1, k)$, gdyż każdemu podziałowi $\pi = \{B_1, \ldots, B_k\}$ zbioru $\{1, \ldots, n-1\}$ odpowiada dokładnie k podziałów w tej klasie powstałych przez dodanie elementu n kolejno do $B_1, B_2, \ldots, B_k$. □

Tablica 3. Liczby Stirlinga drugiego rodzaju $S(n, k)$

n \ k	0	1	2	3	4	5	6	7	8	9	10
0	1	0	0	0	0	0	0	0	0	0	0
1	0	1	0	0	0	0	0	0	0	0	0
2	0	1	1	0	0	0	0	0	0	0	0
3	0	1	3	1	0	0	0	0	0	0	0
4	0	1	7	6	1	0	0	0	0	0	0
5	0	1	15	25	10	1	0	0	0	0	0
6	0	1	31	90	65	15	1	0	0	0	0
7	0	1	63	301	350	140	21	1	0	0	0
8	0	1	127	966	1701	1050	266	28	1	0	0
9	0	1	255	3025	7770	6951	2646	462	36	1	0
10	0	1	511	9330	34105	42525	22827	5880	750	45	1

Liczby $S(n, k)$ dla $0 \leqslant n, k \leqslant 10$ przedstawiono w tabl. 3. Zauważmy, że tablicę tę można traktować – na podobieństwo trójkąta Pascala – jako „trójkąt Stirlinga", w którym każdą wartość, oprócz skrajnych, równych jedności, można otrzymać z liczb występujących bezpośrednio nad nią; dokładniej, jest ona sumą liczby występującej dokładnie nad nią pomnożonej przez k oraz liczby nad nią po lewej stronie.

Oto przykład innej zależności rekurencyjnej związanej z liczbami $S(n, k)$:

TWIERDZENIE 8.4. *Dla* $k \geqslant 2$

$$S(n, k) = \sum_{i=k-1}^{n-1} \binom{n-1}{i} S(i, k-1).$$

Dowód. Niech $X = \{1, \ldots, n\}$ i niech B będzie podzbiorem zbioru X zawierającym element n. Dla każdego takiego zbioru B istnieje dokładnie $S(n-|B|, k-1)$ podziałów $\pi \in \Pi_k(X)$ zawierających B jako jeden z bloków. Zbiór $B \subseteq X$ o b elementach zawierający n możemy wybrać na $\binom{n-1}{b-1}$ sposobów, mamy

zatem

$$S(n, k) = \sum_{b=1}^{n-(k-1)} \binom{n-1}{b-1} S(n-b, k-1) = \sum_{b=1}^{n-(k-1)} \binom{n-1}{n-b} S(n-b, k-1) =$$
$$= \sum_{i=k-1}^{n=1} \binom{n-1}{i} S(i, k-1). \quad \square$$

Fundamentalną własnością liczb Stirlinga drugiego rodzaju jest następujący związek, jaki określają one między wielomianami x^n i $[x]_n$.

TWIERDZENIE 8.5. *Dla każdego* $n \geqslant 0$

(8.8)
$$x^n = \sum_{k=0}^{n} S(n, k)[x]_k.$$

Dowód. Załóżmy najpierw, że x jest nieujemną liczbą całkowitą i policzmy na dwa sposoby liczbę wszystkich funkcji $f\colon A \to B$, gdzie $|A| = n$, $|B| = x$. Z jednej strony, takich funkcji jest x^n (por. twierdzenie 3.1). Z drugiej strony, nasze funkcje możemy sklasyfikować ze względu na obraz $f(A)$. Dla każdego $C \subseteq B$ istnieje dokładnie s_{nk} funkcji $f\colon A \to B$ takich, że $f(A) = C$, przy czym oznaczyliśmy $|C| = k$. Dla każdego k zbiór k-elementowy $C \subseteq B$ możemy wybrać na $\binom{x}{k}$ sposobów. Korzystając ze wzoru (8.3) mamy więc

$$x^n = \sum_{k=0}^{x} \binom{x}{k} s_{nk} = \sum_{k=0}^{x} \frac{[x]_k}{k!} \cdot k!\, S(n, k) = \sum_{k=0}^{n} [x]_k S(n, k)$$

(górny wskaźnik sumowania mogliśmy zmienić z x na n, gdyż $S(n, k) = 0$ dla $k > n$ oraz $[x]_k = 0$ dla $k > x$). Udowodniliśmy więc żądaną równość wielomianów dla nieskończenie wielu wartości zmiennej x. Stąd wynika natychmiast, że wielomiany te są tożsamościowo równe. $\square$

Niech $p_0(x)$, $p_1(x)$, ... będzie dowolnym ciągiem wielomianów takim, że dla każdego i wielomian $p_i(x)$ jest stopnia i. Każdy wielomian $P(x)$ stopnia n można wtedy oczywiście jednoznacznie przedstawić jako $P(x) = \sum_{k=0}^{n} a_k p_k(x)$. Innymi słowy, każdy taki ciąg $p_0(x)$, $p_1(x)$, ... stanowi bazę w przestrzeni liniowej wszystkich wielomianów. W tych terminach wzory (4.11) i (8.8) orzekają po prostu, iż liczby Stirlinga pierwszego i drugiego rodzaju są współczynnikami macierzy przejścia odpowiednio z bazy $1, x, x^2, \ldots$ do bazy $1, [x]_1, [x]_2, \ldots$ i w przeciwną stronę.

Porównując współczynniki przy kolejnych potęgach x po obu stronach równości

$$x^n = \sum_{k=0}^{n} S(n, k)[x]_k = \sum_{k=0}^{n} S(n, k) \sum_{j=0}^{k} s(k, j) x^j =$$
$$= \sum_{k=0}^{n} \sum_{j=0}^{n} S(n, k) s(k, j) x^j = \sum_{j=0}^{n} \sum_{k=0}^{n} S(n, k) s(k, j) x^j$$

otrzymujemy następującą zależność pomiędzy liczbami Stirlinga pierwszego i drugiego rodzaju

$$\sum_{k=0}^{n} S(n, k)s(k, j) = \delta_{nj}, \tag{8.9}$$

gdzie δ_{nj} jest deltą Kroneckera, tzn. $\delta_{nj} = 0$ dla $n \neq j$ i $\delta_{nn} = 1$. Jest to oczywiście również bezpośredni wniosek ze wspomnianej już interpretacji liczb Stirlinga jako współczynników macierzy przejścia między pewnymi bazami przestrzeni liniowej wielomianów.

Na zakończenie tego paragrafu zdefiniujemy tzw. liczby Bella. *Liczbę Bella* B_n określamy jako liczbę wszystkich podziałów zbioru n-elementowego, tzn.

$$B_n = |\Pi(X)|, \qquad \text{gdzie } |X| = n.$$

Tablica 4. Liczby Bella B_n

n	B_n
0	1
1	1
2	2
3	5
4	15
5	52
6	203
7	877
8	4140
9	21147
10	115975
11	678570
12	4213597
13	27644437
14	190899322
15	1382958545
16	10480142147
17	82864869804
18	682076806159
19	5832742205057
20	51724158235372

Oczywiście

$$B_n = \sum_{k=0}^{n} S(n, k).$$

Prostą metodę rekurencyjną wyznaczania liczb Bella daje następujące twierdzenie:

TWIERDZENIE 8.6.

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_i.$$

Dowód. Podzielmy wszystkie podziały zbioru $\{1, \ldots, n+1\}$ na rozłączne klasy w zależności od bloku zawierającego element $n+1$. Taki blok B zawierający i elementów oprócz elementu $n+1$ możemy wybrać na $\binom{n}{i}$ sposobów, przy czym klasa odpowiadająca blokowi B zawiera dokładnie B_{n-i} podziałów, tyle ile jest wszystkich podziałów zbioru $\{1, \ldots, n+1\} \setminus B$. Stąd

$$B_{n+1} = \sum_{i=0}^{n} \binom{n}{i} B_{n-i} = \sum_{i=0}^{n} \binom{n}{n-i} B_{n-i} = \sum_{i=0}^{n} \binom{n}{i} B_i. \quad \square$$

Liczby Bella B_n, $1 \leqslant n \leqslant 20$, przedstawiono w tabl. 4.

§ 9. Skończone ciała zbiorów

Przypomnijmy, że ciałem zbiorów nazywamy dowolną rodzinę $\mathcal{F}$ podzbiorów pewnego zbioru X spełniającą następujące dwa warunki:

$$A \in \mathcal{F} \Rightarrow X \setminus A \in \mathcal{F},$$

$$A \in \mathcal{F} \wedge B \in \mathcal{F} \Rightarrow A \cup B \in \mathcal{F}.$$

Jest oczywiste, że każde ciało zbiorów jest zamknięte również względem przecięcia i różnicy zbiorów; wystarczy zauważyć, iż $A \cap B = X \setminus ((X \setminus A) \cup (X \setminus B))$ oraz $A \setminus B = A \cap (X \setminus B)$. Dla dowolnej rodziny $\mathfrak{M} \subseteq \mathcal{P}(X)$ istnieje najmniejsze ciało $\mathcal{F}(\mathfrak{M})$ zawierające rodzinę $\mathfrak{M}$, jest nim mianowicie część wspólna wszystkich ciał zawierających $\mathfrak{M}$.

Interesować nas będzie głównie przypadek, gdy $\mathfrak{M}$ jest rodziną skończoną. Ustalmy pewne poindeksowanie $M_1, \ldots, M_n$ zbiorów takiej rodziny. Dla dowolnego ciągu zero-jedynkowego $\varepsilon = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ definiujemy

$$S(\varepsilon) = M_1^{\varepsilon_1} \cap \ldots \cap M_n^{\varepsilon_n},$$

gdzie dla każdego $M \subseteq X$ stosujemy oznaczenie $M^0 = M$, $M^1 = X \setminus M$. Zbiory postaci $S(\varepsilon)$ nazywamy *składowymi* rodziny $\mathfrak{M}$ (nie musimy tu, ani w dalszym ciągu zakładać, że zbiory $M_1, \ldots, M_n$ są parami różne — w istocie możemy mówić o składowych dowolnego ciągu podzbiorów zbioru X). Udowodnimy teraz kilka prostych własności składowych.

TWIERDZENIE 9.1. (a) *Jeśli* $\varepsilon \neq \varepsilon'$, *to* $S(\varepsilon) \cap S(\varepsilon') = \emptyset$.
(b) *Sumą wszystkich składowych jest zbiór* X.
(c) *Sumą wszystkich składowych* $S(\varepsilon)$ *takich, że* $\varepsilon_i = 0$, *jest zbiór* M_i.

Dowód. (a) Jeśli $\varepsilon \neq \varepsilon'$, tzn. $\varepsilon_i \neq \varepsilon_i'$ dla pewnego i, to $M_i^{\varepsilon_i} \cap M_i^{\varepsilon_i'} = M_i \cap (X \setminus M_i) = \emptyset$ i w konsekwencji

$$S(\varepsilon) \cap S(\varepsilon') = M_1^{\varepsilon_1} \cap \ldots \cap M_i^{\varepsilon_i} \cap \ldots \cap M_n^{\varepsilon_n} \cap M_1^{\varepsilon_1'} \cap \ldots \cap M_i^{\varepsilon_i'} \cap \ldots \cap M_n^{\varepsilon_n'} = \emptyset.$$

(b) Należy wykazać, że każdy element $x \in X$ należy do pewnej składowej. Ustalmy taki element x i zdefiniujmy

$$\varepsilon_i = \begin{cases} 0, & \text{jeśli } x \in M_i, \\ 1, & \text{jeśli } x \notin M_i. \end{cases}$$

Wtedy $x \in M_i^{\varepsilon_i}$, $1 \leqslant i \leqslant n$, a więc $x \in S(\varepsilon)$, gdzie $\varepsilon = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$.

(c) Zauważmy, że dla każdego ciągu $\varepsilon = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ takiego, że $\varepsilon_i = 0$ mamy

$$S(\varepsilon) = M_1^{\varepsilon_1} \cap \ldots \cap M_{i-1}^{\varepsilon_{i-1}} \cap M_i \cap M_{i+1}^{\varepsilon_{i+1}} \cap \ldots \cap M_n^{\varepsilon_n} \subseteq M_i.$$

Z drugiej strony, dla każdego elementu $x \in M_i$ ciąg $\varepsilon = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle$ zdefiniowany w dowodzie punktu (b) – który ma tę własność, iż $x \in S(\varepsilon)$ – ma zero na i-tej pozycji. □

Wykażemy teraz, że jeśli $\mathfrak{M} \subseteq \mathscr{P}(X)$ jest rodziną skończoną, to najmniejsze ciało zbiorów $\mathscr{F}(\mathfrak{M})$ zawierające $\mathfrak{M}$ jest też skończone.

TWIERDZENIE 9.2. *Jeśli* $|\mathfrak{M}| = n$, *to* $|\mathscr{F}(\mathfrak{M})| \leqslant 2^{2^n}$.

Dowód. Niech $S_1, \ldots, S_m$ będą niepustymi składowymi rodziny $\mathfrak{M}$. Oczywiście $m \leqslant 2^n$, gdyż każda niepusta składowa odpowiada innemu ciągowi zero-jedynkowemu $\langle \varepsilon_1, \ldots, \varepsilon_n \rangle$. Wykażemy, że $\mathscr{F}(\mathfrak{M})$ jest rodziną wszystkich możliwych sum składowych, tzn.

$$\mathscr{F}(\mathfrak{M}) = \{\bigcup_{j \in J} S_j \colon J \subseteq \{1, \ldots, m\}\}.$$

Oznaczmy przez $\mathfrak{N}$ prawą stronę powyższej równości. Aby udowodnić, iż $\mathfrak{N} = \mathscr{F}(\mathfrak{M})$ wystarczy oczywiście stwierdzić następujące trzy fakty:

(a) $\mathfrak{M} \subseteq \mathfrak{N}$,

(b) $\mathfrak{N}$ jest ciałem zbiorów,

(c) $\mathfrak{N} \subseteq \mathscr{F}(\mathfrak{M})$.

Punkt (a) wynika bezpośrednio z twierdzenia 9.1c. Punkt (b) jest również wnioskiem z twierdzenia 9.1, gdyż wobec faktu, iż $\{S_1, \ldots, S_m\}$ jest podziałem zbioru X mamy:

$$\bigcup_{j \in J} S_j \cup \bigcup_{k \in K} S_k = \bigcup_{j \in J \cup K} S_j,$$

$$X \setminus \bigcup_{j \in J} S_j = \bigcup_{j \in \{1, \ldots, m\} \setminus J} S_j.$$

Punkt (c) wreszcie wynika z faktu, że skoro każdą składową, a więc i każdą sumę składowych można otrzymać ze zbiorów $M_1, \ldots, M_n$ za pomocą operacji $\cup$, $\cap$, $\setminus$, to każda taka suma należy do każdego ciała zbiorów zawierającego $\mathfrak{M}$. Liczność ciała $\mathscr{F}(\mathfrak{M})$ jest więc równa liczbie wszystkich podzbiorów $J \subseteq \{1, \ldots, m\}$, a więc $2^m \leqslant 2^{2^n}$. □

Na składowe rodziny $\mathfrak{M} = \{M_1, \ldots, M_n\}$ można jeszcze spojrzeć nieco inaczej. Zbiór M_i generuje podział $\pi_i = \{M_i, X \setminus M_i\}$ i łatwo zauważyć, że podział zbioru

X na składowe wyraża się jako $\pi_1 \wedge \ldots \wedge \pi_n$ (por. twierdzenie 8.1). Nasze poprzednie rozważania przenoszą się w oczywisty sposób na sytuację, gdy podziały π_i są dowolne, niekoniecznie o dwóch blokach. Istotnie, niech danych będzie n podziałów zbioru X: $\pi_i = \{M_i^0, \ldots, M_i^{r_i-1}\}$, $1 \leqslant i \leqslant n$. Powtarzając nasze poprzednie rozumowania można łatwo udowodnić, że składowe rodziny $\mathfrak{M} = \pi_1 \cup \ldots \cup \pi_n$ są postaci

$$S(\varepsilon) = M_1^{\varepsilon_1} \cap \ldots \cap M_n^{\varepsilon_n},$$

gdzie $\varepsilon = \langle \varepsilon_1, \ldots, \varepsilon_n \rangle \in \{0, \ldots, r_1-1\} \times \ldots \times \{0, \ldots, r_n-1\}$. Stąd wniosek, że liczba niepustych składowych nie przekracza $r_1 \ldots r_n$. Podobnie jak poprzednio, zbiór X jest sumą rozłączną wszystkich składowych oraz $M_i^{\varepsilon_j}$ jest dokładnie sumą tych składowych $S(\varepsilon)$, dla których $\varepsilon_i = j$.

Często w praktyce wygodny jest następujący standardowy system numeracji składowych. Definiujemy liczby

$$\begin{aligned} u_1 &= 1, \\ u_2 &= r_1, \\ u_3 &= r_1 r_2, \\ &\ldots\ldots\ldots\ldots \\ u_n &= r_1 r_2 \ldots r_{n-1}, \end{aligned}$$

i każdej niepustej składowej $S(\varepsilon)$, gdzie $0 \leqslant \varepsilon_i < r_i$ dla $1 \leqslant i \leqslant n$, przyporządkowujemy numer

(9.1) $$N(\varepsilon) = \sum_{i=1}^{n} \varepsilon_i u_i.$$

Zauważmy, że jeśli $r_1 = \ldots = r_n = 2$, to ε jest po prostu binarnym rozwinięciem liczby $N(\varepsilon)$. Podobnie, jeśli $r_1 = \ldots = r_n = k > 2$, to $N(\varepsilon)$ odpowiada liczbie reprezentowanej przez ε w systemie pozycyjnym o podstawie k. W przypadku ogólnym, gdy liczby $r_1, \ldots, r_n$ są niekoniecznie równe, mamy do czynienia z „brytyjskim systemem pozycyjnym" (sprzed reformy walutowej funta).

Na zakończenie tego paragrafu podamy przykład podziałów $\pi_1, \ldots, \pi_n$ takich, że wszystkie $r_1 \ldots r_n$ składowe są niepuste; o takich podziałach mówimy, że są *niezależne*. W tym celu przyjmijmy

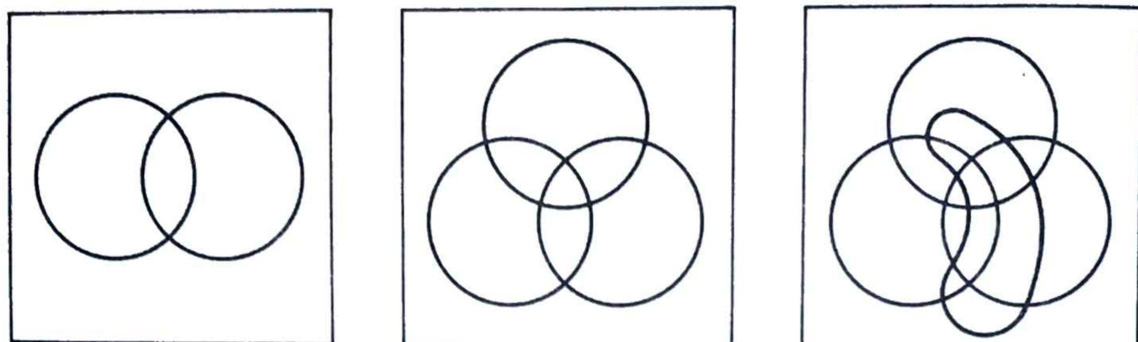
$$\begin{aligned} X &= \{0, \ldots, r_1-1\} \times \ldots \times \{0, \ldots, r_n-1\}, \\ \pi_i &= \{M_i^0, \ldots, M_i^{r_i-1}\}, \quad 1 \leqslant i \leqslant n, \end{aligned}$$

gdzie

$$M_i^j = \{\varepsilon \in X\colon \varepsilon_i = j\}, \quad 1 \leqslant i \leqslant n,\ 0 \leqslant j < r_i.$$

Dla tak zdefiniowanej rodziny podziałów mamy oczywiście $S(\varepsilon) = \{\varepsilon\}$, każda składowa jest więc niepusta. W szczególności, dla $r_1 = \ldots = r_n = 2$, zbiory

$M_1, \ldots, M_n$ o wszystkich 2^n składowych niepustych nazywamy również *niezależnymi*. Rodziny zbiorów niezależnych dla $n = 2, 3, 4$ przedstawiono schematycznie na rys. 9.



Rys. 9. Rodziny zbiorów niezależnych dla $n = 2, 3, 4$. Każdy spójny obszar wewnątrz kwadratu odpowiada składowej

§ 10. Zależności rekurencyjne, funkcje tworzące

W wielu zagadnieniach kombinatorycznych mamy do czynienia z sytuacją, w której poszukiwane rozwiązanie możemy reprezentować przez ciąg liczbowy a_0, a_1, a_2, ... Typowym przykładem jest przypadek, w którym a_n jest liczbą pewnych obiektów kombinatorycznych „wymiaru n" spełniających ograniczenia określone warunkami zadania. Często struktura problemu umożliwia łatwe znalezienie zależności rekurencyjnej określającej a_n jako funkcję ciągu $a_0, \ldots, a_{n-1}$ (najprostszy jest przypadek, w którym ta funkcja zależy jedynie od a_{n-1}), naszym zadaniem zaś jest znalezienie na podstawie tych zależności rekurencyjnych ogólnego wzoru na a_n w jawnej i możliwie zwartej postaci.

Rozważmy następujący prosty przykład. Niech a_n oznacza liczbę permutacji zbioru $\{1, \ldots, n\}$ (przyjmujemy $a_0 = 1$). Zauważmy, że $a_1 = 1$, oraz że $a_n = na_{n-1}$, każdą permutację zbioru $\{1, \ldots, n\}$ możemy bowiem otrzymać z pewnej jednoznacznie określonej permutacji zbioru $\{1, \ldots, n-1\}$ przez wstawienie elementu n na jeden z n możliwych sposobów: przed pierwszy wyraz, między pierwszy a drugi wyraz itd. (permutację zbioru $\{1, \ldots, n\}$ utożsamiamy z ciągiem różnowartościowym długości n). Stąd łatwo już wynika wzór $a_n = n!$.

Zajmiemy się teraz problemem prowadzącym do nieco bardziej skomplikowanej zależności rekurencyjnej. Będzie to klasyczne *zadanie o królikach* rozważane w XIII w. przez Leonarda Fibonacciego z Pizy. Przypuśćmy, że każda nowo narodzona para królików wydaje co miesiąc jedną parę potomstwa, poczynając od drugiego miesiąca życia. Oznaczając przez N, M, D odpowiednio parę królików nowo narodzonych, młodych (jednomiesięcznych) i dojrzałych możemy nasz proces, rozpoczynający się od jednej nowo narodzonej pary, przedstawić następująco:

Stan początkowy N
Po 1 miesiącu M,
Po 2 miesiącach D, N,
Po 3 miesiącach D, M, N,
Po 4 miesiącach D, D, M, N, N,
Po 5 miesiącach D, D, D, M, M, N, N, N,
. . . .

Oznaczmy przez f_n liczbę królików po n miesiącach (przy założeniu, że króliki nie zdychają), oraz przedstawmy f_n jako sumę $f_n^D+f_n^M+f_n^N$ odpowiednio królików dojrzałych, młodych i nowo narodzonych. Dla $n \geqslant 2$ mamy wtedy

(10.1) $$f_n = f_{n-1}+f_n^N = f_{n-1}+f_n^D = f_{n-1}+f_{n-2}.$$

Ostatnia równość wynika stąd, że pary dorosłe po n miesiącach to wszystkie pary po $n-2$ miesiącach i tylko one.

Opiszemy teraz technikę pozwalającą na wyznaczenie ogólnego wzoru na f_n. Technika ta oparta jest na pojęciu tzw. funkcji tworzącej. Funkcje tworzące mają wiele innych zastosowań — niektóre z nich omówimy w tym paragrafie. Stanowią one jedno z podstawowych narzędzi w kombinatorycznych zagadnieniach zliczania.

Funkcją tworzącą dla ciągu liczb zespolonych a_0, a_1, a_2, ... nazywamy następującą funkcję zmiennej zespolonej x:

(10.2) $$A(x) = \sum_{n=0}^{\infty} a_n x^n.$$

Czasami używa się też nazwy *funkcja tworząca zwyczajna*, dla odróżnienia od funkcji tworzącej eksponencjalnej wprowadzonej w dalszym ciągu tego paragrafu i innych rodzajów funkcji tworzących rozważanych w rozdziale 3.

W niniejszym paragrafie wszystkie rozważane przez nas ciągi a_0, a_1, a_2, ... będą miały tę własność, że szereg (10.2) jest zbieżny w pewnym otoczeniu punktu 0 (tzn. dla wszystkich x takich, że $|x| < r$, gdzie $r > 0$). W takim przypadku z analizy matematycznej wiadomo, że suma $A(x)$ rozważanego szeregu jest funkcją analityczną w tym otoczeniu i współczynniki a_n wyrażają się jednoznacznie wzorem

(10.3) $$a_n = \frac{A^{(n)}(0)}{n!}, \quad n = 0, 1, 2, \ldots,$$

gdzie $A^{(n)}(0)$ oznacza wartość n-tej pochodnej funkcji $A(x)$ dla $x=0$ (p. np. Kuratowski [1]). Wzory (10.1) i (10.2) określają odpowiedniość wzajemnie jednoznaczną między funkcjami analitycznymi w otoczeniu zera i ciągami a_0, a_1, a_2, ... takimi, że szereg (10.2) jest zbieżny w otoczeniu zera. Co więcej, elementarnym faktem z analizy matematycznej jest to, że jeśli

$$A(x) = \sum_{n=0}^{\infty} a_n x^n, \quad B(x) = \sum_{n=0}^{\infty} b_n x^n$$

są funkcjami analitycznymi w otoczeniu zera, to iloczyn przez dowolną liczbę $cA(x)$, suma $A(x)+B(x)$, iloczyn $A(x)\cdot B(x)$ i pochodna $A'(x)$ są funkcjami analitycznymi w otoczeniu zera, przy czym

$$cA(x) = \sum_{n=0}^{\infty} ca_n x^n, \tag{10.4}$$

$$A(x)+B(x) = \sum_{n=0}^{\infty} (a_n+b_n) x^n, \tag{10.5}$$

$$A(x)\cdot B(x) = \sum_{n=0}^{\infty} \Big(\sum_{k=0}^{n} a_k b_{n-k}\Big) x^n, \tag{10.6}$$

$$A'(x) = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n. \tag{10.7}$$

W istocie, stosując funkcje tworzące do problemów zliczania nigdy nie obliczamy wartości szeregu (10.2) dla konkretnej wartości zmiennej x, wyznaczamy jedynie współczynniki funkcji powstałej z pewnych funkcji tworzących przez zastosowanie działania sumy, iloczynu i różniczkowania. W rozdziale 3 pokażemy, że możemy nie zajmować się zupełnie problemem zbieżności funkcji tworzących, traktując je jako tzw. szeregi formalne, a więc jedynie jako wygodną formalną reprezentację ich współczynników. Przy takim podejściu wzory (10.4)–(10.7) traktujemy jako definicje działań na szeregach formalnych. Zanim jednak ściśle uzasadnimy taką czysto algebraiczną teorię funkcji tworzących, pozostajemy przy podejściu analitycznym.

Powróćmy do zależności rekurencyjnej (10.1) i rozważmy funkcję tworzącą

$$F(x) = \sum_{n=0}^{\infty} f_n x^n. \tag{10.8}$$

Załóżmy, że szereg ten jest zbieżny w pewnym otoczeniu zera. Wtedy na mocy naszych zależności rekurencyjnych otrzymujemy

$$F(x) = \sum_{n=0}^{\infty} f_n x^n = f_0+f_1 x+\sum_{n=2}^{\infty} f_n x^n = 1+x+\sum_{n=2}^{\infty} (f_{n-1}+f_{n-2}) x^n =$$

$$= 1+x+x\sum_{n=1}^{\infty} f_n x^n + x^2 \sum_{n=0}^{\infty} f_n x^n = 1+xF(x)+x^2F(x) = 1+(x+x^2)F(x),$$

a stąd

$$F(x) = \frac{1}{1-x-x^2}.$$

Łatwo sprawdzić, że współczynniki powyższej funkcji analitycznej w otoczeniu zera istotnie spełniają zależności $f_0=f_1=1$, $f_n=f_{n-1}+f_{n-2}$ dla $n\geqslant 0$, co uzasadnia nasze założenie o zbieżności szeregu (10.8) w otoczeniu zera. Wystarczy teraz wyznaczyć współczynniki rozwinięcia funkcji $(1-x-x^2)^{-1}$, tzn. rozwinąć ją w szereg Maclaurina. W tym celu znajdujemy najpierw pierwiastki równania

$1-x-x^2=0$ i otrzymujemy rozkład

$$1-x-x^2=(1-\alpha x)(1-\beta x),$$

gdzie

$$\alpha=(1+\sqrt{5})/2, \qquad \beta=(1-\sqrt{5})/2.$$

Stosujemy teraz metodę współczynników nieoznaczonych do znalezienia współczynników A, B takich, że

$$\frac{1}{(1-\alpha x)(1-\beta x)}=\frac{A}{1-\alpha x}+\frac{B}{1-\beta x}=\frac{A+B-(A\beta+B\alpha)x}{(1-\alpha x)(1-\beta x)}.$$

Porównując współczynniki w liczniku otrzymujemy $A+B=1$, $A\beta+B\alpha=0$ a stąd

$$A=\frac{\alpha}{\alpha-\beta}, \qquad B=\frac{-\beta}{\alpha-\beta}.$$

Stosując teraz znany wzór na sumę nieskończonego postępu geometrycznego:

$$\sum_{n=0}^{\infty} p^n=\frac{1}{1-p} \qquad (|p|<1)$$

otrzymujemy

$$F(x)=\frac{A}{1-\alpha x}+\frac{B}{1-\beta x}=A\sum_{n=0}^{\infty}\alpha^n x^n+B\sum_{n=0}^{\infty}\beta^n x^n=\sum_{n=0}^{\infty}\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta}x^n,$$

i ostatecznie

$$f_n=\frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1}-\left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right].$$

Liczby f_n nazywamy *liczbami Fibonacciego*.

Użytą tu metodę można uogólnić na dowolne liniowe równania rekurencyjne o stałych współczynnikach, tzn. zależności postaci

$$a_n=A_1 a_{n-1}+A_2 a_{n-2}+\ldots+A_k a_{n-k}, \qquad n\geqslant k,$$

gdzie k, $A_1, \ldots, A_k$ są ustalone (por. zad. 66).

Znajdziemy teraz funkcje tworzące dla kilku rozważanych przez nas już wcześniej ciągów.

Zaczniemy od liczb Stirlinga pierwszego rodzaju. Funkcją tworzącą dla ciągów $a_0, a_1, a_2, \ldots$, gdzie $a_k=s(n,k)$, jest oczywiście wielomian $[x]_n$; wynika to z samej definicji liczb $s(n,k)$ (por. (4.11)).

Funkcją tworzącą dla ciągu 0, 1, 2, 3, ... jest

$$\sum_{n=0}^{\infty} nx^n=x\sum_{n=1}^{\infty} nx^{n-1}=x\frac{d}{dx}\sum_{n=0}^{\infty} x^n=x\frac{d}{dx}(1-x)^{-1}=x(1-x)^{-2}.$$

Ważną rolę odgrywa funkcja tworząca dla współczynników dwumiennych $\binom{n}{k}$ (n ustalone). Na podstawie wzoru (5.1) mamy:

$$\sum_{k=0}^{\infty} \binom{n}{k} x^k = \sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n.$$

Rozważmy interpretację kombinatoryczną tego wzoru analogiczną do omawianej przy okazji wzoru (5.1). Niech $X = \{e_1, \ldots, e_n\}$ będzie pewnym zbiorem n-elementowym. W iloczynie $(1+x)^n = (1+x)\ldots(1+x)$ i-ty czynnik $1+x$ możemy traktować jako odpowiadający elementowi e_i i reprezentujący dwie możliwe liczby wystąpień tego elementu w podzbiorze: zero razy (składnik $x^0 = 1$) lub jeden raz (składnik $x^1 = x$). Oczywiście, każdy podzbiór zbioru X określony jest jednoznacznie przez podanie liczby wystąpień w nim każdego z elementów $e_1, \ldots, e_n$, a więc przez wybór składnika z każdego czynnika iloczynu $(1+x)\ldots(1+x)$. Składnik rozwinięcia odpowiadający takiemu wyborowi ma oczywiście swój udział równy jedności we współczynniku przy x^k, gdzie k jest licznością naszego podzbioru.

Rozumowanie to przenosi się w oczywisty sposób na sytuację, w której liczba wystąpień elementu w podzbiorze może być większa od jedności, tzn. na zbiory z powtórzeniami. Niech na przykład $X = (3*a_1, 1*a_2, 2*a_3)$ i oznaczmy przez c_k liczbę podzbiorów k-elementowych tego zbioru z powtórzeniami. Wtedy

$$\sum_{k=0}^{\infty} c_k x^k = (1+x+x^2+x^3)(1+x)(1+x+x^2) =$$

$$= 1+3x+5x^2+6x^3+5x^4+3x^5+x^6.$$

Na liczbę wystąpień elementu e_i można nakładać dowolne ograniczenia. Na przykład, jeśli liczba tych wystąpień ma być niezerowa, to odpowiadający czynnik ma postać

$$(x+x^2+x^3+\ldots) = x(1-x)^{-1},$$

jeśli ma być parzysta, to czynnik ten jest równy

$$(1+x^2+x^4+\ldots) = (1-x^2)^{-1},$$

jeśli nieparzysta, to

$$(x+x^3+x^5+\ldots) = x(1-x^2)^{-1}$$

itd. Obserwacje te prowadzą w oczywisty sposób do następującego ogólnego twierdzenia:

TWIERDZENIE 10.1. *Niech $X = \{e_1, \ldots, e_n\}$ będzie zbiorem n-elementowym i oznaczmy przez c_k liczbę k-elementowych zbiorów z powtórzeniami A o elementach z X takich, że dla $i = 1, \ldots, n$ współczynnik repetycji elementu e_i w A należy do zbioru*

$$\{r_{i1}, r_{i2}, \ldots\} \quad (0 \leqslant r_{i1} < r_{i2} < \ldots).$$

Wtedy funkcja tworząca dla ciągu $c_0, c_1, c_2, \ldots$ jest równa

$$C(x) = \sum_{k=0}^{\infty} c_k x^k = (x^{r_{11}} + x^{r_{12}} + \ldots)(x^{r_{21}} + x^{r_{22}} + \ldots)\ldots(x^{r_{n1}} + x^{r_{n2}} + \ldots). \quad \square$$

W szczególności, jeśli nie nakładamy żadnych ograniczeń na liczbę wystąpień każdego z elementów, to funkcja tworząca ma postać

$$(1+x+x^2+\ldots)\ldots(1+x+x^2+\ldots) = (1-x)^{-1}\ldots(1-x)^{-1} = (1-x)^{-n}.$$

Rozwińmy tę funkcję w szereg Maclaurina. Mamy

$$\frac{d^k}{dx^k}(1-x)^{-n} = (-n)(-n-1)\ldots(-n-k+1)(1-x)^{-n-k}(-1)^k = [n]^k(1-x)^{-n-k},$$

a więc

$$(1-x)^{-n} = \sum_{k=0}^{\infty} \frac{[n]^k}{k!} x^k = \sum_{k=0}^{\infty} \binom{n+k-1}{k} x^k,$$

co stanowi jeszcze jeden dowód twierdzenia 6.1.

Zajmiemy się obecnie zliczeniem liczby ciągów określonej długości o zadanych ograniczeniach na liczbę wystąpień poszczególnych elementów. Wygodnym narzędziem do tego celu będzie *funkcja tworząca eksponencjalna* określona dla danego ciągu $a_0, a_1, a_2, \ldots$ jako

$$B(x) = \sum_{n=0}^{\infty} \frac{a_n}{n!} x^n.$$

Prawdziwy jest natępujący analogon twierdzenia 10.1:

TWIERDZENIE 10.2. *Niech $X = \{e_1, \ldots, e_n\}$ będzie zbiorem n-elementowym i oznaczmy przez c_k liczbę ciągów długości k takich, że dla $i = 1, \ldots, n$ liczba wystąpień elementu e_i należy do zbioru*

$$\{r_{i1}, r_{i2}, \ldots\} \quad (0 \leqslant r_{i1} < r_{i2} < \ldots).$$

Wtedy funkcja tworząca eksponencjalna dla ciągu $c_0, c_1, c_2, \ldots$ jest równa

$$C(x) = \sum_{k=0}^{\infty} \frac{c_k}{k!} x^k = \left(\frac{x^{r_{11}}}{r_{11}!} + \frac{x^{r_{12}}}{r_{12}!} + \ldots\right)\left(\frac{x^{r_{21}}}{r_{21}!} + \frac{x^{r_{22}}}{r_{22}!} + \ldots\right)\ldots\left(\frac{x^{r_{n1}}}{r_{n1}!} + \frac{x^{r_{n2}}}{r_{n2}!} + \ldots\right).$$

Dowód. Oznaczmy przez $D(x) = \sum_{k=0}^{\infty} d_k x^k$ iloczyn szeregów po prawej stronie. Podobnie jak przy zliczaniu podzbiorów z powtórzeniami współczynnik d_k jest równy sumie

$$\sum \frac{1}{r_{1i_1}!} \cdot \frac{1}{r_{2i_2}!} \cdot \ldots \cdot \frac{1}{r_{ni_n}!} = \frac{1}{k!} \sum \frac{k!}{r_{1i_1}! \ldots r_{ni_n}!},$$

gdzie sumowanie przebiega po wszystkich ciągach $i_1, \ldots, i_n$ takich, że $r_{1i_1} + \ldots + r_{ni_n} = k$. Lecz każdy składnik sumy po prawej stronie to nic innego jak liczba ciągów długości k zawierających dokładnie r_{1i_1} wystąpień elementu e_1, r_{2i_2} – wystąpień elementu e_2 itd. (por. twierdzenie 5.1). Suma po prawej stronie jest więc równa liczbie wszystkich ciągów długości k jakie zliczamy, i w konsekwencji $c_k = d_k$, $k = 0, 1, \ldots$ □

Zilustrujemy to twierdzenie na kilku przykładach. Jeśli na liczbę wystąpień elementu e_i nie narzucamy żadnych organiczeń, to zliczamy po prostu wszystkie ciągi długości k o elementach ze zbioru n-elementowego, czyli wszystkie funkcje ze zbioru k-elementowego w zbiór n-elementowy:

$$C(x) = \left(1 + \frac{x}{1!} + \frac{x^2}{2!} + \ldots\right)^n = (e^x)^n = e^{nx} = \sum_{k=0}^{\infty} \frac{(nx)^k}{k!} = \sum_{k=0}^{\infty} \frac{n^k x^k}{k!}.$$

Stąd $c_k = n^k$, w pełnej zgodności z twierdzeniem 3.1.

Jeśli każdy element występuje w ciągu co najwyżej raz, a więc gdy zliczamy wszystkie funkcje różnowartościowe ze zbioru k-elementowego w zbiór n-elementowy, to

$$C(x) = \left(1 + \frac{x}{1!}\right)^n = (1+x)^n = \sum_{k=0}^{\infty} \binom{n}{k} x^k = \sum_{k=0}^{\infty} \frac{[n]_k}{k!} x^k$$

i $c_k = [n]_k$, co stanowi inny dowód twierdzenia 3.2.

Na zakończenie rozważymy przypadek, gdy każdy element występuje w ciągu co najmniej raz. Odpowiada to oczywiście zliczaniu wszystkich funkcji ze zbioru k-elementowego na zbiór n-elementowy. Mamy wtedy

$$C(x) = \left(\frac{x}{1!} + \frac{x^2}{2!} + \ldots\right)^n = (e^x - 1)^n = \sum_{j=0}^{n} \binom{n}{j} e^{jx} (-1)^{n-j} =$$
$$= \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} \sum_{k=0}^{\infty} \frac{(jx)^k}{k!} = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} j^k x^k.$$

Stąd otrzymujemy wzór

$$c_k = \sum_{j=0}^{n} \binom{n}{j} (-1)^{n-j} j^k = \sum_{j=0}^{n} (-1)^j \binom{n}{j} (n-j)^k,$$

znany już z twierdzenia 7.3.

Zauważmy jeszcze, że z powyższych zależności – zliczając tym razem funkcje ze zbioru n-elementowego na k-elementowy i korzystając z zależności (8.3) – otrzymujemy funkcję tworzącą eksponencjalną dla liczb Stirlinga drugiego rodzaju $S(n, k)$ (k ustalone):

$$(e^x-1)^k = \sum_{n=0}^{\infty} s_{nk} \frac{x^n}{n!} = \sum_{n=0}^{\infty} S(n, k) k! \frac{x^n}{n!},$$

czyli

$$\sum_{n=0}^{\infty} S(n, k) \frac{x^n}{n!} = \frac{(e^x-1)^k}{k!}.$$

§ 11. Podziały liczby

Zajmiemy się obecnie następującym problemem: Na ile sposobów można daną liczbę n zapisać w postaci sumy

$$n = b_1 + \ldots + b_k$$

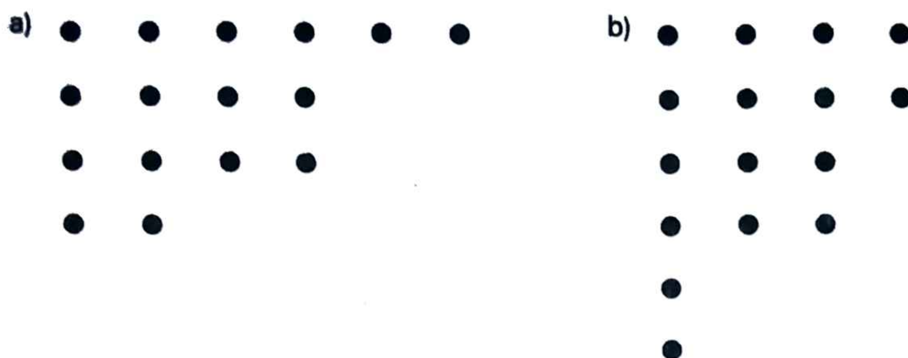
o składnikach całkowitych dodatnich. Jeśli rozkłady różniące się jedynie kolejnością składników uważamy za różne, to zagadnienie nie jest zbyt interesujące. Liczba takich rozkładów na k składników i na dowolną liczbę składników jest bowiem równa, jak łatwo się przekonać, odpowiednio $\binom{n-1}{k-1}$ i 2^{n-1} (p. zad. 69). Znacznie ciekawszy jest przypadek, w którym utożsamiamy rozkłady różniące się jedynie kolejnością składników. W dalszym ciągu będziemy dokonywali zawsze tego utożsamienia i klasę rozkładów równoważnych będziemy reprezentowali przez rozkład o nierosnących składnikach. Formalnie, *podziałem liczby n na k składników* będziemy nazywali ciąg liczb całkowitych $\langle b_1, \ldots, b_k \rangle$ taki, że $b_1 \geqslant b_2 \geqslant \ldots \geqslant b_k > 0$ oraz $b_1 + \ldots + b_k = n$. Podział taki zapisujemy zwykle symbolicznie jako $n = b_1 + \ldots + b_k$. Liczbę wszystkich podziałów liczby n na k składników oznaczamy przez $P(n, k)$, a liczbę wszystkich podziałów liczby n na dowolną liczbę składników – przez $P(n)$ (przyjmujemy $P(0, 0) = P(0) = 1$). Oczywiście

$$P(n) = \sum_{k=0}^{n} P(n, k).$$

Bardzo pomocnym pojęciem przy badaniu podziałów liczby jest tzw. diagram Ferrersa. *Diagram Ferrersa* dla podziału $n = b_1 + \ldots + b_k$ składa się z k wierszy odpowiadających składnikom podziału, przy czym i-ty wiersz składa się z b_i punktów (p. rys. 10). Podamy teraz parę przykładów zastosowania techniki diagramów Ferrersa.

Twierdzenie 11.1. *Dla $n \geqslant k \geqslant 0$*

$$P(n, k) = \sum_{i=0}^{k} P(n-k, i). \tag{11.1}$$



Rys. 10. Diagram Ferrersa (a) podziału $16=6+4+4+2$, (b) sprzężonego względem niego podziału $16=4+4+3+3+1+1$

Dowód. Wystarczy zauważyć, że operacja usuwania pierwszej kolumny diagramu Ferrersa ustala odpowiedniość wzajemnie jednoznaczną pomiędzy wszystkimi podziałami liczby n na k składników a wszystkimi składnikami liczby $n-k$ na co najwyżej k składników. □

Łatwo zauważyć, że zależność rekurencyjna (11.1) wraz z oczywistymi wzorami

$$P(n, k) = 0 \quad \text{dla } n < k,$$
$$P(n, n) = 1 \quad \text{dla } n \geqslant 0,$$
$$P(n, 0) = 0 \quad \text{dla } n > 0.$$

określa jednoznacznie wartości $P(n, k)$ dla dowolnych n, k.

Podział sprzężony względem podziału $n = b_1 + \ldots + b_k$ określamy jako podział $n = b_1^* + \ldots + b_k^*$, gdzie

$$b_i^* = |\{j\colon 1 \leqslant j \leqslant k \wedge b_j \geqslant i\}| = \max\{j\colon 1 \leqslant j \leqslant k \wedge b_j \geqslant i\}.$$

Zauważmy, że podział sprzężony, to nic innego jak podział określony przez transpozycję (zmianę roli wierszy i kolumn) w diagramie Ferrersa (p. rys. 10). Transpozycja diagramu Ferrersa określa odpowiedniość wzajemnie jednoznaczną między podziałami liczby n na k składników a podziałami tej liczby o największym składniku równym k. Odnotujmy ten fakt:

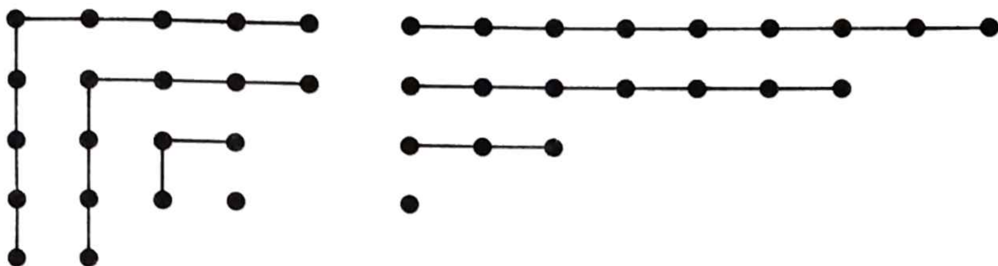
TWIERDZENIE 11.2. *Liczba podziałów liczby n na k składników jest równa liczbie podziałów liczby n o największym składniku równym k.* □

Podział równy podziałowi sprzężonemu względem siebie nazywamy *samosprzężonym*. Użycie techniki diagramów Ferrersa pozwala na łatwe udowodnienie następującego twierdzenia.

TWIERDZENIE 11.3. *Liczba podziałów samosprzężonych liczby n jest równa liczbie podziałów liczby n na składniki nieparzyste parami różne.*

Dowód. Odpowiedniość między podziałami obu typów jest pokazana na rys. 11. Podziałowi samosprzężonemu $n = b_1 + \ldots + b_k$ odpowiada podział $n = c_1 + \ldots + c_p$, gdzie $c_i = 2b_i - 2i + 1$, przy czym wiersz diagramu Ferrersa odpowiadający

składnikowi c_i możemy traktować jako powstały z tych punktów i-tego wiersza i i-tej kolumny diagramu Ferrersa podziału $n = b_1 + \ldots + b_k$, które są połączone linią na rys. 11. □



Rys. 11. Wzajemnie jednoznaczna odpowiedniość między podziałami samosprzężonymi a podziałami na składniki nieparzyste parami różne

Mamy też fakt następujący:

TWIERDZENIE 11.4. *Liczba podziałów liczby n na składniki parami różne jest równa liczbie podziałów liczby n na składniki nieparzyste.*

Dowód. Wykażemy odpowiedniość wzajemnie jednoznaczną między podziałami, o których mowa w twierdzeniu. Rozważmy dowolny podział liczby n na składniki nieparzyste $a_1, \ldots, a_p$, w których składnik a_i występuje r_i razy, $i = 1, \ldots, p$. Niech

$$r_i = 2^{q_1} + 2^{q_2} + \ldots \quad (q_1 > q_2 > \ldots)$$

będzie przedstawieniem binarnym liczby r_i. Suma naszego podziału nie ulegnie zmianie, jeśli zastąpimy r_i składników a_i przez parami różne składniki

$$a_i 2^{q_1}, \; a_i 2^{q_2}, \; \ldots$$

Dokonując takiej zamiany dla $i = 1, \ldots, p$ i porządkując otrzymane składniki w ciąg nierosnący, otrzymujemy pewien podział liczby n na składniki parami różne. Wynika to z faktu, iż każda liczba ma jednoznaczne przedstawienie postaci $a2^q$, gdzie a jest nieparzyste i $q \geqslant 0$. Łatwo zauważyć, że transformacji odwrotnej można dokonać przedstawiając w postaci $a2^q$ (a nieparzyste, $q \geqslant 0$) każdy ze składników podziału na składniki parami różne, następnie grupując składniki według „czynnika nieparzystego" a, i wreszcie zamieniając każdą taką grupę $a2^{q_1}$, $a2^{q_2}, \ldots$ $(q_1 > q_2 > \ldots)$ na $r = 2^{q_1} + 2^{q_2} + \ldots$ składników równych a. Nasza transformacja określa więc odpowiedniość wzajemnie jednoznaczną pomiędzy podziałami na składniki parami różne a podziałami na składniki nieparzyste. □

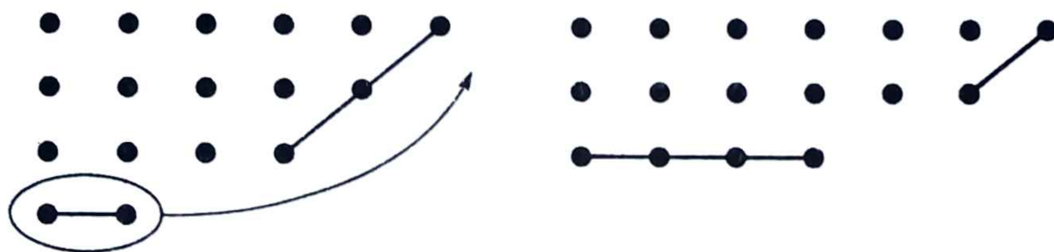
Oznaczmy przez $E(n)$ i $O(n)$ liczbę podziałów liczby n na odpowiednio parzystą i nieparzystą liczbę składników parami różnych. Ostatnim przykładem zastosowania techniki diagramów Ferrersa jaki tu podamy jest dowód następującego twierdzenia.

TWIERDZENIE 11.5 (Euler).

$$E(n)-O(n) = \begin{cases} (-1)^j, & \textit{jeśli } n \textit{ jest postaci } (3k^2 \pm k)/2, \\ 0, & \textit{w przeciwnym przypadku.} \end{cases}$$

Dowód (Franklin [1]). Dla danego podziału $n = b_1 + \ldots + b_k$, gdzie $b_1 > \ldots > b_k$ wprowadźmy dwa parametry:

$$b = b_k, \quad t = \max\{j\colon b_j = b_1 + 1 - j\}.$$



Rys. 12. Do dowodu twierdzenia Eulera ($b = 2$, $t = 3$)

Parametry te są licznościami odpowiednio *podstawy* diagramu Ferrersa, tzn. jego ostatniego wiersza, oraz *przekątnej*, tzn. prawego górnego ograniczenia diagramu Ferrersa (p. rys. 12). Określimy teraz transformację, która przyporządkowuje podziałowi liczby n na parami różne składniki, podział tej samej liczby na o jeden większą lub o jeden mniejszą liczbę parami różnych składników. Jeśli $b < t$, lub też $b = t$ oraz podstawa i przekątna są rozłączne, to nasza transformacja polega na utworzeniu z podstawy nowej przekątnej, tzn. na usunięciu podstawy i dodaniu po jednym punkcie na koniec każdego z pierwszych b wierszy diagramu Ferrersa (p. rys. 12). Jeśli $b > t+1$, lub też $b > t$ oraz podstawa i przekątna są rozłączne, to tworzymy z przekątnej nową podstawę, tzn. usuwamy po jednym punkcie z końca każdego z pierwszych b wierszy diagramu Ferrersa i dodajemy nowy wiersz liczności b. Zauważmy, że w ten sposób określiliśmy naszą transformację dla wszystkich podziałów na parami różne składniki, z wyjątkiem podziałów o diagramie Ferrersa, w którym podstawa ma punkt wspólny z przekątną, przy czym oznaczając liczbę wierszy — równą w naszym przypadku liczności przekątnej — przez k, mamy $b = k$ lub $b = k+1$. Suma podziału wynosi w takim przypadku odpowiednio

$$n = k+(k+1)+ \ldots +(2k-1) = (3k^2-k)/2$$

lub

$$n = (k+1)+(k+2)+ \ldots +2k = (3k^2+k)/2.$$

Łatwo zauważyć, że nasza transformacja jest inwolucją na klasie wszystkich podziałów, dla których jest określona, tzn. wykonując ją dwukrotnie otrzymujemy podział wyjściowy. Stąd już oczywisty wniosek, że wśród podziałów na parami

różne składniki nie będących postaci

(11.2) $$n = (2k-1)+(2k-2)+ \ldots +k$$

ani też

(11.3) $$n = 2k+(2k-1)+ \ldots +(k+1)$$

określa ona odpowiedniość wzajemnie jednoznaczną między podziałami na parzystą i nieparzystą liczbę składników. Wystarczy teraz zauważyć, że dla n postaci $(3k^2 \pm k)/2$ istnieje jeden dodatkowy podział na k składników postaci (11.2) lub (11.3), który nie ma swojego odpowiednika wśród podziałów liczby n o przeciwnej parzystości liczby składników. □

Podobnie jak w przypadku podziałów zbioru (por. § 8) *typem* podziału $n = b_1 + \ldots + b_k$ będziemy nazywali ciąg $\langle \lambda_1, \ldots, \lambda_n \rangle$ taki, że λ_i jest liczbą składników równych i w tym podziale. Oczywiście

(11.4) $$\lambda_1 + 2\lambda_2 + \ldots + n\lambda_n = n.$$

W odróżnieniu od podziałów zbioru, typ podziału liczby wyznacza oczywiście ten podział jednoznacznie. Liczbę $P(n)$ możemy więc interpretować jako liczbę rozwiązań równania (11.4) w liczbach całkowitych nieujemnych $\lambda_1, \ldots, \lambda_n$, liczbę $P(n, k)$ zaś jako liczbę tych rozwiązań, które spełniają dodatkowo warunek $\lambda_1 + \ldots + \lambda_n = k$.

Oznaczmy przez $P_h(n)$ liczbę podziałów liczby n na składniki nie przekraczające h i niech $\varphi_h(x)$ będzie funkcją tworzącą dla ciągu $P_h(0)$, $P_h(1)$, ...

Twierdzenie 11.6.

$$\varphi_h(x) = \sum_{n=0}^{\infty} P_h(n)\,x^n =$$
$$= (1+x+x^2+x^3+ \ldots)(1+x^2+x^4+x^6+ \ldots)\ldots(1+x^h+x^{2h}+x^{3h}+ \ldots) =$$
$$= (1-x)^{-1}(1-x^2)^{-1}\ldots(1-x^h)^{-1}.$$

Dowód. Zgodnie ze wzorem na iloczyn szeregów, prawa strona jest sumą składników postaci

$$x^{\lambda_1}x^{2\lambda_2}\ldots x^{h\lambda_h} = x^{\lambda_1+2\lambda_2+\ldots+h\lambda_h}$$

(λ_i jest numerem wyrazu wybranego z i-tego szeregu). Współczynnik przy x^n jest więc równy liczbie ciągów $\langle \lambda_1, \ldots, \lambda_h \rangle$ takich, że $\lambda_1 + 2\lambda_2 + \ldots + h\lambda_h = n$, a więc, zgodnie z naszymi poprzednimi uwagami, jest on równy $P_h(n)$. □

Można wykazać, że ciąg funkcji analitycznych $\varphi_1(x)$, $\varphi_2(x)$, ... jest zbieżny jednostajnie w pewnym otoczeniu zera do pewnej funkcji analitycznej $\varphi(x)$ będącej funkcją tworzącą dla ciągu $P(0)$, $P(1)$, ..., tzn. że zachodzi wzór

$$\sum_{n=0}^{\infty} P(n)\,x^n = \prod_{i=1}^{\infty} (1-x^i)^{-1}$$

(por. zad. 71). Do wzoru tego powrócimy jeszcze w rozdziale 3.

§ 12. Geometrie skończone

Jak wiadomo, każde ciało skończone liczy p^m elementów, gdzie p jest liczbą pierwszą a $m \in N$. Co więcej, dla każdego p i m istnieje, z dokładnością do izomorfizmu, dokładnie jedno ciało o $q = p^m$ elementach, oznaczane zwykle przez $GF(q)$. Podstawowe wiadomości o ciałach skończonych Czytelnik może znaleźć w Dodatku.

Każda przestrzeń liniowa n-wymiarowa nad ciałem $GF(q)$ jest oczywiście izomorficzna z przestrzenią $V(n, q)$ złożoną z ciągów $\langle x_1, \ldots, x_n \rangle$, $x_i \in GF(q)$, z naturalnymi działaniami:

$$\langle x_1, \ldots, x_n \rangle + \langle y_1, \ldots, y_n \rangle = \langle x_1 + y_1, \ldots, x_n + y_n \rangle,$$

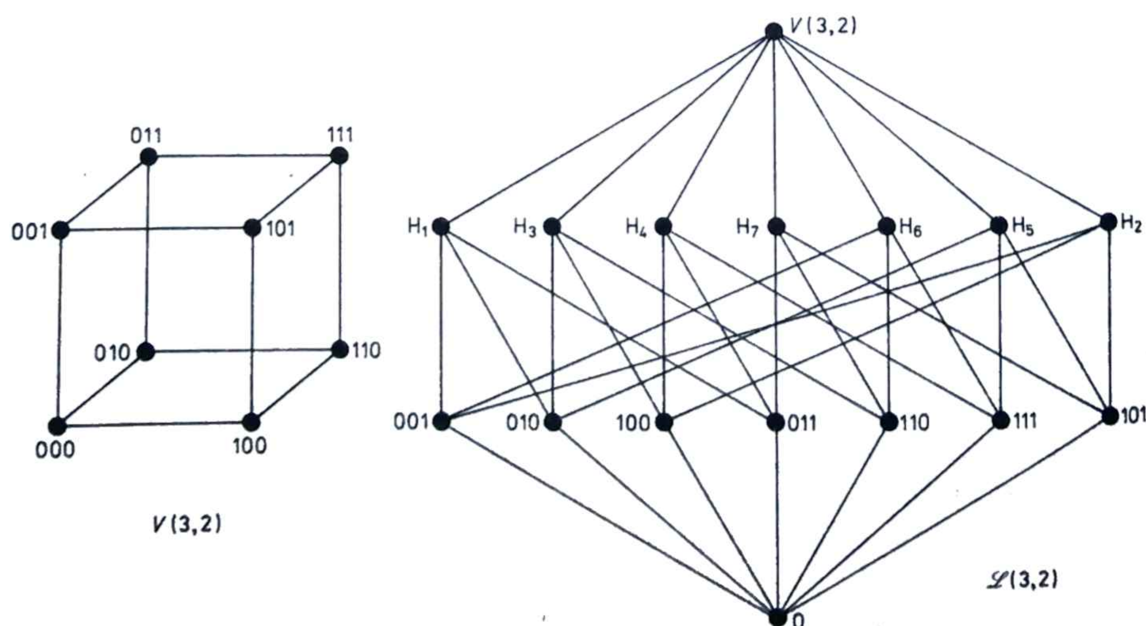
$$\lambda \langle x_1, \ldots, x_n \rangle = \langle \lambda x_1, \ldots, \lambda x_n \rangle.$$

Rozważmy zbiór wszystkich podprzestrzeni liniowych przestrzeni $V(n, q)$ częściowo uporządkowany przez relację zawierania. Łatwo sprawdzić, że zbiór ten jest kratą, przy czym

$$Z \wedge T = Z \cap T,$$

$$Z \vee T = \{z + t\colon\ z \in Z \wedge t \in T\}.$$

Zerem i jedynką w tej kracie są odpowiednio podprzestrzeń zerowa, której jedynym elementem jest $0 = \langle 0, \ldots, 0 \rangle$, oraz cała przestrzeń $V(n, q)$. Kratę tę będziemy oznaczali przez $\mathscr{L}(n, q)$. Zauważmy, że ranga elementu Z tej kraty, to nic innego jak wymiar podprzestrzeni Z (oznaczamy go zwykle przez $\dim Z$).



Rys. 13. Przestrzeń liniowa $V(3, 2)$ i krata jej podprzestrzeni $\mathscr{L}(3, 2)$

Na rys. 13 przedstawiono schematycznie przestrzeń liniową $V(3, 2)$ oraz kratę $\mathscr{L}(3, 2)$. Podprzestrzenie jednowymiarowe przestrzeni $V(3, 2)$ mają postać $\{0, a\}$, gdzie a jest niezerowym elementem przestrzeni $V(3, 2)$. Elementy rangi 1 w $\mathscr{L}(3, 2)$ można więc identyfikować z elementami niezerowymi przestrzeni. Podprzestrzenie dwuwymiarowe są następujące (każda z poniższych podprzestrzeni jest zbiorem elementów $\langle x_1, x_2, x_3\rangle$ spełniających równanie wypisane po prawej stronie):

$$
\begin{aligned}
&H_1 = \{000, 001, 010, 011\}, && x_1 &&= 0,\\
&H_2 = \{000, 001, 100, 101\}, && x_2 &&= 0,\\
&H_3 = \{000, 010, 100, 110\}, && x_3 &&= 0,\\
&H_4 = \{000, 011, 100, 111\}, && x_2+x_3 &&= 0,\\
&H_5 = \{000, 010, 101, 111\}, && x_1+x_3 &&= 0,\\
&H_6 = \{000, 001, 110, 111\}, && x_1+x_2 &&= 0,\\
&H_7 = \{000, 011, 101, 110\}, && x_1+x_2+x_3 &&= 0.
\end{aligned}
\tag{12.1}
$$

Podprzestrzenie H_1, H_2, H_3 odpowiadają bokom sześcianu z rys. 13 zawierającym 000, podprzestrzenie H_4, H_5, H_6 natomiast „płaszczyznom" przechodzącym przez krawędź sześcianu zawierającą 000 i równoległą do niej krawędź zawierającą 111. Podprzestrzeni H_7 nie można nadać takiej prostej interpretacji, która używałaby intuicji związanych z geometryczną strukturą zwykłej przestrzeni euklidesowej $\mathbf{R}^3$.

Podobnie jak w przypadku innych rozważanych przez nas zbiorów częściowo uporządkowanych, będzie nas interesowała liczba elementów rangi k w $\mathscr{L}(n, q)$. Liczbę tę oznaczamy przez $\binom{n}{k}_q$ i nazywamy *współczynnikiem Gaussa.*

TWIERDZENIE 12.1.

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

(*przyjmujemy* $\binom{n}{0}_q = 1$).

Dowód. Policzymy dwoma sposobami wszystkie bazy $\langle e_1, \dots, e_k\rangle$ wszystkich k-wymiarowych podprzestrzeni przestrzeni $V(n, q)$ (bazę traktujemy jako ciąg, w którym kolejność elementów jest istotna). Z jednej strony, element e_1 takiej bazy możemy wybrać na q^n-1 sposobów, element e_2 na q^n-q sposobów, i ogólnie: element e_i na q^n-q^{i-1} sposobów, e_i może bowiem być dowolnym elementem przestrzeni $V(n, q)$ nie należącym do $(i-1)$-wymiarowej podprzestrzeni rozpiętej przez $e_1, \dots, e_{i-1}$. Daje to $(q^n-1)(q^n-q)\dots(q^n-q^{k-1})$ możliwości. Z drugiej strony, na mocy podobnego rozumowania, dla każdej spośród $\binom{n}{k}_q$ podprzestrzeni k-wymiarowych przestrzeni $V(n, q)$ istnieje dokładnie $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$

baz, które ją rozpinają. Stąd liczba wszystkich baz wszystkich podprzestrzeni k-wymiarowych jest równa $\binom{n}{k}_q (q^k-1)(q^k-q)\dots(q^k-q^{k-1})$. Wystarczy teraz porównać wyniki otrzymane tymi dwoma sposobami. □

(12.2) $$\sum_{k=0}^{n} \binom{n}{k}_q.$$

Można łatwo wykazać, że podane w twierdzeniu 12.1 wyrażenie określające $\binom{n}{k}_q$ dąży do $\binom{n}{k}$ przy $q \to 1$. Okazuje się, że wiele tożsamości związanych ze współczynnikami Gaussa daje znane tożsamości dla współczynników dwumiennych przy podstawieniu $q = 1$. Co więcej, tożsamości dla współczynników Gaussa mają często podobne dowody „kombinatoryczne” jak odpowiednie tożsamości dla współczynników dwumiennych. Przytoczymy teraz niektóre z nich.

(12.3) $$\binom{n}{k}_q = \binom{n}{n-k}_q.$$

Wzór ten wynika bezpośrednio z drugiego wyrażenia na $\binom{n}{k}_q$ w twierdzeniu 12.1. Pokażemy jednak inny dowód, który przy okazji powie znacznie więcej o strukturze kraty $\mathscr{L}(n, q)$. Przypomnijmy najpierw pewne elementarne fakty z algebry liniowej. Przestrzenią dualną względem danej przestrzeni liniowej W nad ciałem K nazywamy przestrzeń liniową W^* złożoną z wszystkich funkcjonałów liniowych f: $W \to K$ z działaniami określonymi w naturalny sposób:

$$(f+g)(w) = f(w)+g(w),$$

$$(\lambda f)(w) = \lambda f(w).$$

Każda baza $\langle e_1, \dots, e_n\rangle$ przestrzeni W określa bazę dualną $e_1^*, \dots, e_n^*$ w W^*, gdzie $e_i^*(e_j) = \delta_{ij}$ (delta Kroneckera). W przypadku przestrzeni skończenie wymiarowych przestrzenie W i W^* są więc izomorficzne. Niech teraz $W = V(n, q)$. Dla każdej podprzestrzeni $T \subseteq W$ oznaczmy przez $T^\perp$ zbiór tych funkcjonałów f, których jądro $f^{-1}(0)$ zawiera T. Oczywiście $T^\perp$ jest podprzestrzenią przestrzeni W^*, przy czym

$$T \subseteq S \Rightarrow T^\perp \supseteq S^\perp,$$

tzn. przyporządkowanie $T \mapsto T^\perp$ określa monotoniczne odwzorowanie kraty $\mathscr{L}(n, q)$ w kratę dualną $\mathscr{L}^*(n, q)$ (tzn. kratę powstałą z $\mathscr{L}(n, q)$ przez odwrócenie częściowego porządku). Pozostawimy Czytelnikowi sprawdzenie, że odwzorowanie to jest izomorfizmem (por. zad. 73). Udowodniliśmy więc, że krata $\mathscr{L}(n, q)$ jest samodualna, tzn. izomorficzna z kratą względem niej dualną. Wzór (12.3) wynika więc z faktu, iż element rangi k w $\mathscr{L}(n, q)$ ma rangę $n-k$ w $\mathscr{L}^*(n, q)$.

Udowodnimy obecnie analogon tożsamości związanej z trójkątem Pascala (p. wzór (5.12)).

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{n}_q. \tag{12.4}$$

Dowód. Ustalmy w $V(n, q)$ dowolną podprzestrzeń jednowymiarową U. Zbiór wszystkich podprzestrzeni k-wymiarowych przestrzeni $V(n, q)$ rozpada się na dwie rozłączne klasy: tych, które zawierają U, i tych, które podprzestrzeni U nie zawierają. Na mocy samodualności kraty $\mathscr{L}(n, q)$ liczność pierwszej klasy wynosi tyle, ile jest podprzestrzeni $(n-k)$-wymiarowych przestrzeni $(n-1)$-wymiarowej, czyli

$$\binom{n-1}{n-k}_q = \binom{n-1}{(n-1)-(n-k)}_q = \binom{n-1}{k-1}_q,$$

co pokrywa się z pierwszym składnikiem po prawej stronie wzoru (12.4). Wyznaczymy teraz liczność drugiej klasy. Mamy $|U| = q$, a więc możemy wybrać bazę podprzestrzeni k-wymiarowej nie zawierającej U na

$$(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1}) = q^k(q^{n-1}-1)(q^{n-1}-q)\dots(q^{n-1}-q^{k-1})$$

sposobów. Lecz każda taka podprzestrzeń jest wyznaczona przez dokładnie $(q^k-1)(q^k-q)\dots(q^k-q^{k-1})$ różnych baz. Stąd liczność drugiej klasy wynosi

$$\frac{q^k(q^{n-1}-1)(q^{n-1}-q)\dots(q^{n-1}-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})} = q^k\binom{n-1}{k}_q,$$

co kończy dowód. □

Udowodnimy teraz tożsamość, którą w pewnym sensie możemy uważać za analogon wzoru dwumiennego (5.1).

TWIERDZENIE 12.3.

$$x^n = \sum_{k=0}^{n} \binom{n}{k}_q (x-1)(x-q)\dots(x-q^{k-1}). \tag{12.5}$$

Dowód. Wystarczy wykazać tę tożsamość dla nieskończenie wielu wartości zmiennej x — stąd oczywiście wyniknie równość wielomianów po obu stronach. Obliczymy dwoma sposobami liczbę odwzorowań liniowych $f\colon V(n, q) \to X$, gdzie X jest przestrzenią liniową o x elementach (x jest więc postaci q^m, $m = 1, 2, \dots$). Z jednej strony, każde takie odwzorowanie jest jednoznacznie wyznaczone przez wybranie jednego z x możliwych obrazów każdego z elementów pewnej ustalonej bazy $\langle e_1, \dots, e_n\rangle$ przestrzeni $V(n, q)$, a więc wszystkich odwzorowań jest x^n (lewa strona wzoru (12.5)). Z drugiej strony, policzmy ile jest odwzorowań liniowych o ustalonym jądrze T wymiaru k. Ustalmy w tym celu bazę $\langle e_1, \dots, e_n\rangle$ przestrzeni $V(n, q)$ taką, że $\langle e_1, \dots, e_k\rangle$ jest bazą podprzestrzeni T. Każde od-

wzorowanie liniowe f: $V(n, q) \to X$ takie, że $f^{-1}(0) = T$ jest wyznaczone jednoznacznie przez wybranie liniowo niezależnych obrazów elementów $e_{k+1}, \ldots, e_n$. Takich wyborów jest oczywiście $(x-1)(x-q)\ldots(x-q^{k-1})$. Dla każdego k jądro wymiaru k możemy wybrać na $\binom{n}{k}_q$ sposobów, prawa strona wzoru (12.5) wyraża więc również liczbę wszystkich odwzorowań liniowych z $V(n, q)$ w X. □

Podobieństwo wzoru (12.5) do wzoru dwumiennego polega na tym, że przy $q \to 1$ prawa strona przechodzi w sumę $\sum_{k=0}^{n} \binom{n}{k}(x-1)^k$, w której łatwo rozpoznajemy rozwinięcie wyrażenia $((x-1)+1)^n$.

Zauważmy, że w istocie twierdzenie 12.3 mówi, iż współczynniki Gaussa określają przejście z bazy $(x-1)(x-q)\ldots(x-q^{k-1})$, $k = 0, 1, \ldots$, do bazy x^k, $k = 0, 1, \ldots$ Współczynniki przejścia w przeciwną stronę poznamy w następnym rozdziale.

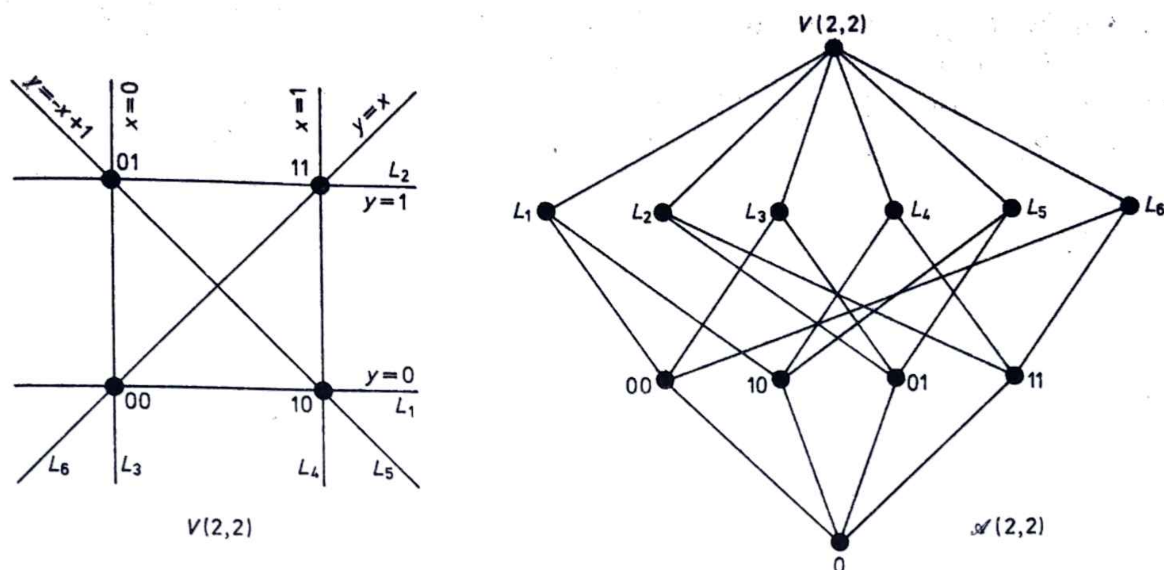
Niech T będzie dowolną przestrzenią liniową, Z zaś dowolną jej podprzestrzenią. Relacja binarna $\underset{Z}{\equiv}$ określona na T wzorem

$$a \underset{Z}{\equiv} b \Leftrightarrow a-b \in Z$$

jest oczywiście relacją równoważności. Jej klasy abstrakcji nazywamy *warstwami* przestrzeni T względem podprzestrzeni Z. Zgodnie z definicją każda taka warstwa ma postać

$$a+Z = \{a+z:\ z \in Z\},$$

przy czym $a+Z = b+Z$ wtedy i tylko wtedy, gdy $a-b \in Z$. Łatwo też sprawdzić, że zbiór $A \subseteq T$ jest warstwą względem podprzestrzeni Z wtedy i tylko wtedy, gdy $-a+A = Z$ dla pewnego $a \in A$ (lub równoważnie, dla wszystkich $a \in A$). Wymiar warstwy $a+Z$ definiujemy jako wymiar podprzestrzeni Z. Zauważmy, że przecięcie dowolnej rodziny $\langle A_i \rangle_{i \in I}$ warstw (niekoniecznie względem tej samej podprzestrzeni) jest albo puste, albo jest też warstwą. Istotnie, załóżmy, że $a \in \bigcap_{i \in I} A_i$. Przecięcie podprzestrzeni liniowych $\bigcap_{i \in I} (-a+A_i) = S$ jest podprzestrzenią liniową i oczywiście $\bigcap_{i \in I} A_i = a+S$. Stąd wniosek, że zbiór wszystkich warstw względem dowolnych podprzestrzeni przestrzeni T, uzupełniony o zbiór pusty, tworzy kratę, w której $A \wedge B = A \cap B$, $A \vee B$ natomiast jest przecięciem wszystkich warstw zawierających $A \cup B$. Można też łatwo wykazać, że jeśli T jest przestrzenią liniową nad ciałem K, to $A \vee B$ jest zbiorem wszystkich elementów postaci $\lambda_1 a_1 + \ldots + \lambda_m a_m$, gdzie $m \geq 1$, $\lambda_1, \ldots, \lambda_m \in K$, $\lambda_1 + \ldots + \lambda_m = 1$ i $a_1, \ldots, a_m \in A \cup B$ (p. zad. 76). Kratę warstw n-wymiarowej przestrzeni liniowej nad ciałem $GF(q)$ będziemy oznaczali przez $\mathscr{A}(n, q)$. Na rysunku 14 przedstawiono schematycznie przestrzeń liniową $V(2, 2)$ oraz kratę $\mathscr{A}(2, 2)$.



Rys. 14. Przestrzeń liniowa $V(2, 2)$ i krata jej warstw $\mathscr{A}(2, 2)$

Kratę $\mathscr{A}(n, q)$ opisuje się często w bardziej „geometrycznych" terminach, używając pojęcia tzw. *geometrii afinicznej* $AG(n, q)$ (używana jest też czasem nazwa *geometria euklidesowa* i oznaczenie $EG(n, q)$). O elementach przestrzeni $V(n, q)$ (które możemy oczywiście utożsamiać z elementami rangi 1 w $\mathscr{A}(n, q)$) mówimy, że są *punktami* geometrii $AG(n, q)$, natomiast o warstwach jednowymiarowych przestrzeni $V(n, q)$ (tzn. o elementach rangi 2 w $\mathscr{A}(n, q)$), że są *prostymi* tej geometrii. Jeśli punkt a należy do prostej L, to mówimy też, że prosta L *przechodzi* przez punkt a, lub że jest *incydentna* z a. Zauważmy, że przez każde dwa różne punkty a, b geometrii $AG(n, q)$ przechodzi dokładnie jedna prosta — jest nią mianowicie prosta

$$L = \{\lambda a + (1-\lambda) b\colon \lambda \in GF(q)\}.$$

Ogólnie, przez *podprzestrzeń k-wymiarową* geometrii $AG(n, q)$ rozumiemy dowolną warstwę k-wymiarową przestrzeni $V(n, q)$, tzn. element rangi $k+1$ w $\mathscr{A}(n, q)$. Łatwo sprawdzić, że zbiór $A \subseteq V(n, q)$ jest podprzestrzenią geometrii $AG(n, q)$ wtedy i tylko wtedy, gdy dla każdych dwóch różnych punktów $a, b \in A$ prosta przechodząca przez te punkty jest zawarta w A (p. zad. 77).

Zajmiemy się obecnie konstrukcją tzw. *geometrii rzutowej* $PG(n, q)$. Rozważmy w tym celu przestrzeń liniową $V(n+1, q)$. O dowolnych dwóch elementach $a, b \in V(n+1, q) \setminus \{0\}$ będziemy mówili, że są *proporcjonalne*, jeśli $a = \lambda b$ dla pewnego $\lambda \in GF(q)$ (tzn. jeśli a, b są liniowo zależne). Proporcjonalność jest oczywiście relacją równoważności na $V(n+1, q) \setminus \{0\}$. Klasy abstrakcji tej relacji — możemy o nich myśleć jako o „kierunkach" w $V(n+1, q)$ — przyjmujemy jako *punkty* geometrii rzutowej $PG(n, q)$. Jeśli T jest podprzestrzenią k-wymiarową przestrzeni $V(n+1, q)$, to $T \setminus \{0\}$ jest oczywiście sumą rozłączną pewnej liczby naszych klas abstrakcji. O zbiorze tych klas abstrakcji — a więc punktów

geometrii $PG(n, q)$ – będziemy mówili, że tworzy *podprzestrzeń* $(k-1)$-wymiarową geometrii $PG(n, q)$ wyznaczoną przez T (przyjmujemy, że $\emptyset$ jest podprzestrzenią wymiaru -1 geometrii $PG(n, q)$). W szczególności, podprzestrzenie wymiaru 1 geometrii $PG(n, q)$, zwane *prostymi* tej geometrii, są wyznaczone przez podprzestrzenie dwuwymiarowe przestrzeni $V(n+1, q)$. Zgodnie z tą definicją istnieje odpowiedniość wzajemnie jednoznaczna między podprzestrzeniami geometrii $PG(n, q)$ a podprzestrzeniami przestrzeni $V(n+1, q)$, która, co więcej, ustala izomorfizm kraty podprzestrzeni geometrii $PG(n, q)$ (gdzie częściowy porządek odpowiada inkluzji) z kratą $\mathscr{L}(n+1, q)$.

Szczególnie prosty jest przypadek $q = 2$. Możemy bowiem wtedy utożsamiać punkty geometrii $PG(n, q)$ z niezerowymi elementami przestrzeni $V(n+1, q)$.

Łatwo sprawdzić, że podobnie jak w przypadku geometrii afinicznej przez każde dwa różne punkty geometrii rzutowej przechodzi dokładnie jedna prosta; wynika to z faktu, iż każde dwie różne podprzestrzenie jednowymiarowe przestrzeni liniowej rozpinają pewną podprzestrzeń dwuwymiarową.

Wyznaczymy obecnie liczbę podprzestrzeni danego wymiaru dla $AG(n, q)$ i $PG(n, q)$.

TWIERDZENIE 12.4. (a) *Liczba podprzestrzeni k-wymiarowych geometrii $AG(n, q)$, tzn. liczba elementów rangi $k+1$ w $\mathscr{A}(n, q)$, jest równa $q^{n-k}\binom{n}{k}_q$.*

(b) *Liczba podprzestrzeni k-wymiarowych geometrii $PG(n, q)$, tzn. liczba elementów rangi $k+1$ w $\mathscr{L}(n+1, q)$, jest równa $\binom{n+1}{k+1}_q$.*

Dowód. (a) Każda podprzestrzeń k-wymiarowa T przestrzeni $V(n, q)$ liczy q^k elementów i indukuje podział przestrzeni $V(n, q)$ na q^{n-k} warstw przestrzeni $V(n, q)$ względem T. Podprzestrzeń k-wymiarową możemy wybrać na $\binom{n}{k}_q$ sposobów, stąd liczba wszystkich warstw k-wymiarowych jest równa $q^{n-k}\binom{n}{k}_q$. Punkt (b) jest oczywisty. □

W przypadku $n = 2$ termin „geometria" zastępujemy terminem „płaszczyzna", i mówimy o *płaszczyźnie afinicznej* $AG(2, q)$ i *płaszczyźnie rzutowej* $PG(2, q)$.

Płaszczyzna $AG(2, q)$ zawiera q^2 punktów $\langle x, y\rangle$ $(x, y \in GF(q))$, oraz, zgodnie z twierdzeniem 12.4,

$$q^{2-1}\binom{n}{1}_q = q\frac{q^2-1}{q-1} = q^2+q$$

prostych. Łatwo zauważyć, że jest to q prostych „pionowych" (o „nieskończonym nachyleniu") o równaniach

$$x = c \qquad (c \in GF(q)),$$

oraz, dla każdego $a \in GF(q)$, po q prostych o „nachyleniu” a, o równaniach

$$y = ax + b \qquad (b \in GF(q)).$$

Oczywiście, każde dwie różne proste albo się przecinają w dokładnie jednym punkcie, albo są rozłączne. Jeśli dwie proste L_1, L_2 są rozłączne lub równe, to mówimy, że są one *równoległe* i piszemy $L_1 \| L_2$.

Odnotujmy następujące trzy własności płaszczyzny $AG(2, q)$:

PA1. *Przez każde dwa różne punkty przechodzi dokładnie jedna prosta.*

PA2. *Dla każdej prostej L i każdego punktu p nie leżącego na tej prostej istnieje dokładnie jedna prosta L' przechodząca przez p i równoległa do L.*

PA3. *Istnieją cztery różne punkty, z których żadne trzy nie leżą na jednej prostej.*

Własności PA1 i PA3 są oczywiste, własność PA2 („postulat Euklidesa”) sprawdzamy rozważając jako L' odpowiednią prostą o tym samym — być może nieskończonym — nachyleniu co L i zauważając ponadto, iż proste o różnych nachyleniach zawsze się przecinają.

Własności PA1, PA2, PA3 mogą służyć jako system aksjomatów w abstrakcyjnej definicji płaszczyzny afinicznej. Będziemy mianowicie mówili, że para $\langle X, \mathscr{B} \rangle$, gdzie X jest zbiorem (którego elementy nazywamy *punktami*), zaś $\mathscr{B}$ pewną rodziną podzbiorów zbioru X (zwanych *prostymi*), jest *płaszczyzną afiniczną*, jeśli spełnione są warunki PA1, PA2, PA3. Oczywiście każda płaszczyzna $AG(2, q)$ jest szczególnym przypadkiem takiego abstrakcyjnego pojęcia płaszczyzny afinicznej, można jednak wykazać (por. M. Hall [3]), że istnieją skończone płaszczyzny afiniczne — tzn. płaszczyzny afiniczne o skończonym zbiorze punktów — które nie są izomorficzne z żadną płaszczyzną $AG(2, q)$ (przez izomorfizm płaszczyzn $\langle X_1, \mathscr{B}_1 \rangle$, $\langle X_2, \mathscr{B}_2 \rangle$ rozumiemy oczywiście istnienie odwzorowania wzajemnie jednoznacznego f zbioru X_1 na zbiór X_2 takiego, że $L \in \mathscr{B}_1 \Leftrightarrow f(L) \in \mathscr{B}_2$).

Zauważmy, że w dowolnej płaszczyźnie afinicznej relacja równoległości (tzn. równości lub rozłączności) jest relacją równoważności na zbiorze prostych. Jest ona oczywiście zwrotna i symetryczna, wystarczy więc wykazać, że jest przechodnia. W tym celu załóżmy, że $L_1 \| L_2$ i $L_2 \| L_3$. Jeśli $L_1 = L_2$ lub $L_2 = L_3$, to oczywiście $L_1 \| L_3$. Niech więc $L_1 \neq L_2$ oraz $L_2 \neq L_3$. Przypuśćmy, że $p \in L_1 \cap L_3$. Zgodnie z PA2 istnieje dokładnie jedna prosta przechodząca przez p i równoległa do L_2. Stąd $L = L_1 = L_3$.

Klasy abstrakcji relacji równoległości nazywamy *kierunkami*. Oczywiście w przypadku płaszczyzny $AG(2, q)$ mamy $q+1$ kierunków, każdy złożony z prostych o tym samym, być może nieskończonym nachyleniu (p. rys. 14, gdzie można rozpoznać płaszczyznę $AG(2, 2)$).

W podobny sposób możemy wprowadzić abstrakcyjne pojęcie *płaszczyzny rzutowej* jako pary $\langle X, \mathscr{B} \rangle$, gdzie X jest zbiorem elementów zwanych *punktami*, $\mathscr{B}$ rodziną jego podzbiorów, zwanych *prostymi*, oraz spełnione są następujące warunki:

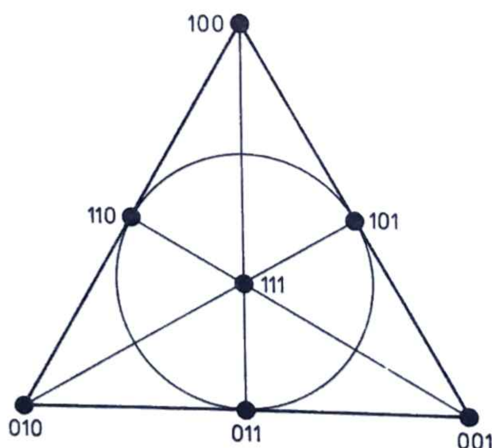
PR1. *Przez każde dwa różne punkty przechodzi dokładnie jedna prosta.*

PR2. *Każde dwie różne proste przechodzą przez dokładnie jeden wspólny punkt.*

PR3. *Istnieją cztery różne punkty, z których żadne trzy nie leżą na jednej prostej.*

Oczywiście, płaszczyzna $PG(2, q)$ jest szczególnym przypadkiem takiego abstrakcyjnego pojęcia płaszczyzny rzutowej. Własność PR2 dla płaszczyzny $PG(2, q)$ wynika z oczywistego faktu, iż przecięcie każdych dwóch różnych podprzestrzeni dwuwymiarowych w $V(3, q)$ jest pewną podprzestrzenią jednowymiarową (jest to też wniosek z PR1 i samodualności kraty $\mathscr{L}(3, q)$).

Przypatrzmy się bliżej płaszczyźnie $PG(2, 2)$. Jej punkty możemy utożsamiać z siedmioma niezerowymi elementami przestrzeni $V(3, 2)$, jej siedem prostych otrzymujemy natomiast usuwając element zerowy z siedmiu podprzestrzeni dwuwymiarowych $H_1, \ldots, H_7$ przestrzeni $V(3, 2)$ wyznaczonych już poprzednio przy konstrukcji kraty $\mathscr{L}(3, 2)$ (p. rys. 13). Płaszczyznę $PG(2, 2)$ (jest ona także zwana *płaszczyzną Fano*) przedstawiono schematycznie na rys. 15. Jej proste są reprezentowane przez odcinki łączące odpowiednie trójki punktów, z wyjątkiem prostej $\{011, 101, 110\}$, która jest reprezentowana przez okrąg.



Rys. 15. Płaszczyzna rzutowa $PG(2,2)$ (płaszczyzna Fano)

Można wykazać, że istnieją skończone płaszczyzny rzutowe — tzn. płaszczyzny rzutowe o skończonej liczbie punktów — które nie są izomorficzne z żadną płaszczyzną $PG(2, q)$ (p. np. M. Hall [3]).

Wprowadzimy obecnie pojęcie rzędu płaszczyzny rzutowej. Do tego celu będzie nam potrzebny następujący lemat.

LEMAT 12.5. *Dla każdej skończonej płaszczyzny rzutowej istnieje liczba m taka, że każda prosta liczy dokładnie $m+1$ punktów i przez każdy punkt przechodzi dokładnie $m+1$ prostych.*

Dowód. Rozważmy dowolne dwie proste L_1, L_2. Udowodnimy, że $|L_1| = |L_2|$. Wykażemy najpierw, że istnieje punkt $p \notin L_1 \cup L_2$. Istotnie, niech a, b, c, d będą

czterema punktami, których istnienie orzeka PR3. Jeśli wszystkie one należą do $L_1 \cup L_2$, to bez zmniejszenia ogólności możemy przyjąć, że $a, b \in L_1 \setminus L_2$ oraz $c, d \in L_2 \setminus L_1$. Niech L_3, L_4 będą prostymi przechodzącymi odpowiednio przez a, c i b, d, oraz niech p będzie punktem przecięcia prostych L_3 i L_4. Nie może być $p \in L_1$, gdyż wtedy, wobec PR1, byłoby $L_1 = L_3$ i w konsekwencji $c \in L_1$, wbrew naszemu założeniu. Podobnie niemożliwy jest przypadek $p \in L_2$; a więc $p \notin L_1 \cup L_2$.

Dla każdego punktu $a \in L_1$ istnieje, wobec PR1, dokładnie jedna prosta przechodząca przez p i a. Na mocy PR2 prosta ta przecina L_2 w dokładnie jednym punkcie – oznaczmy go przez $f(a)$. Określona w ten sposób funkcja $f\colon L_1 \to L_2$ wyznacza oczywiście odwzorowanie wzajemnie jednoznaczne punktów prostej L_1 na punkty prostej L_2.

Niech teraz p będzie dowolnym punktem, L zaś dowolną prostą nie przechodzącą przez ten punkt (istnienie takiej prostej jest łatwym wnioskiem z PR3). Dla każdej prostej K przechodzącej przez p oznaczmy przez $g(K)$ punkt przecięcia prostej K z prostą L. Wobec PR1 i PR2 określona w ten sposób funkcja g jest odwzorowaniem wzajemnie jednoznacznym zbioru prostych przechodzących przez punkt p na punkty prostej L. □

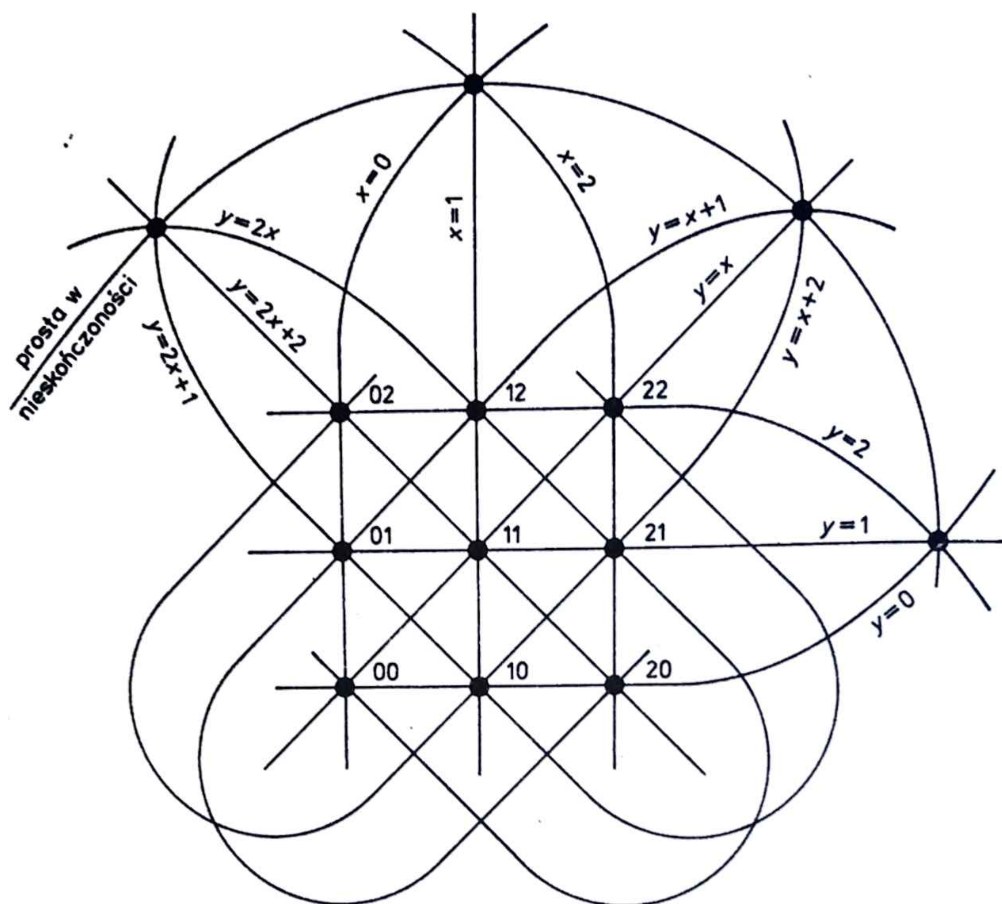
Liczbę m, o której mowa w lemacie 12.5 nazywamy *rzędem* płaszczyzny rzutowej. Oczywiście $PG(2, q)$ jest płaszczyzną rzędu q.

Pokażemy obecnie, jak z danej skończonej płaszczyzny afinicznej $\langle X, \mathscr{B}\rangle$ skonstruować pewną płaszczyznę rzutową. Niech $\mathscr{P}_1, \ldots, \mathscr{P}_r$ będą kierunkami w $\langle X, \mathscr{B}\rangle$. Dla każdej takiej klasy $\mathscr{P}_i$ rozważmy pewien nowy punkt p_i (tzw. „punkt w nieskończoności"). Oznaczmy $L = \{p_1, \ldots, p_r\}$ („prosta w nieskończoności") oraz $\mathscr{P}_i^* = \{P \cup \{p_i\}\colon P \in \mathscr{P}_i\}$ dla $i = 1, \ldots, r$. Wtedy $\langle X \cup L, \mathscr{P}_1^* \cup \ldots \cup \mathscr{P}_r^* \cup \{L\}\rangle$ jest płaszczyzną rzutową; pozostawiamy Czytelnikowi łatwe sprawdzenie faktu, iż spełnione są warunki PR1, PR2, PR3. Na rysunku 16 pokazano konstrukcję płaszczyzny rzutowej rzędu 3 z płaszczyzny afinicznej $AG(2, 3)$.

Zauważmy, że z naszej konstrukcji i z lematu 12.5 wynika, że w dowolnej skończonej płaszczyźnie afinicznej $\langle X, \mathscr{B}\rangle$ każda prosta ma tę samą liczność. Liczność tę nazywamy *rzędem* płaszczyzny afinicznej $\langle X, \mathscr{B}\rangle$. Zgodnie z tą definicją, rząd danej płaszczyzny afinicznej jest taki sam jak rząd płaszczyzny rzutowej otrzymanej z niej przez opisaną powyżej konstrukcję. Oczywiście $AG(2, q)$ jest płaszczyzną rzędu q.

TWIERDZENIE 12.6. *Każda płaszczyzna afiniczna rzędu m zawiera dokładnie m^2 punktów oraz $m+1$ kierunków liczących po m prostych, w sumie m^2+m prostych. Każda prosta zawiera dokładnie m punktów, a przez każdy punkt przechodzi $m+1$ prostych.*

Dowód. Niech $\langle X, \mathscr{B}\rangle$ będzie płaszczyzną afiniczną rzędu m. Skonstruujmy z niej, w uprzednio opisany sposób, płaszczyznę rzutową rzędu m. Liczba kierunków w $\langle X, \mathscr{B}\rangle$ jest równa liczności prostej w nieskończoności naszej płaszczyzny rzutowej, tzn. $m+1$, zgodnie z lematem 12.5. Liczność każdego kierunku jest równa m, tyle ile jest, wobec lematu 12.5, w naszej płaszczyźnie rzutowej prostych,



Rys. 16. Konstrukcja płaszczyzny rzutowej rzędu 3 z płaszczyzny afinicznej $AG(2, 3)$

różnych od prostej w nieskończoności, przechodzących przez punkt w nieskończoności. Stąd liczba wszystkich prostych jest równa $m(m+1) = m^2+m$. Liczność każdej prostej jest równa m, zgodnie z definicją rzędu płaszczyzny afinicznej. Przez każdy punkt płaszczyzny $\langle X, \mathscr{B}\rangle$, zgodnie z naszą konstrukcją, przechodzi tyle samo prostych co w płaszczyźnie rzutowej, czyli $m+1$. Mamy wreszcie $|X| = m^2$, wystarczy bowiem zauważyć, że każdy kierunek jest podziałem zbioru X na m bloków liczności m. □

Łatwo podać również konstrukcję odwrotną względem poprzednio opisanej. Jeśli $\langle X, \mathscr{B}\rangle$ jest dowolną płaszczyzną rzutową rzędu m, to wybierając jako „prostą w nieskończoności" dowolną prostą $L \in \mathscr{B}$, usuwając ją z $\mathscr{B}$ oraz usuwając dla każdej z pozostałych prostych jej punkt przecięcia z L otrzymujemy, jak łatwo sprawdzić, pewną płaszczyznę afiniczną rzędu m. Z wiązki prostych przechodzących przez dowolny „punkt w nieskończoności" otrzymujemy przy tej konstrukcji pewien kierunek. Uzyskujemy stąd, wobec twierdzenia 12.6 i lematu 12.5, następujący wniosek:

Twierdzenie 12.7. *Każda płaszczyzna rzutowa rzędu m zawiera dokładnie* m^2+m+1 *punktów i* m^2+m+1 *prostych. Każda prosta zawiera dokładnie* $m+1$ *punktów, a przez każdy punkt przechodzi* $m+1$ *prostych.*

Jak pokażemy w rozdziale 7, nie dla każdej liczby naturalnej $m \geqslant 2$ istnieje płaszczyzna rzutowa rzędu m. Z opisanych przez nas tu konstrukcji wynika jednak następujący fakt.

TWIERDZENIE 12.8. *Płaszczyzna rzutowa rzędu m istnieje wtedy i tylko wtedy, gdy istnieje płaszczyzna afiniczna rzędu m.*

Zadania

1 (*Wzory de Morgana*). Udowodnić, że dla dowolnej indeksowanej rodziny $\langle A_i \rangle_{i \in I}$ podzbiorów zbioru X

$$X \setminus \bigcup_{i \in I} A_i = \bigcap_{i \in I} (X \setminus A_i),$$

$$X \setminus \bigcap_{i \in I} A_i = \bigcup_{i \in I} (X \setminus A_i).$$

2. Oznaczmy przez $A \oplus B$ różnicę symetryczną zbiorów A i B, tzn. $A \oplus B = (A \cup B) \setminus (A \cap B)$. Wykazać, że

$$A \oplus A = \emptyset, \qquad A \oplus \emptyset = A,$$

$$A \oplus B = B \oplus A,$$

$$(A \oplus B) \oplus C = A \oplus (B \oplus C),$$

$$A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C),$$

oraz że dla każdego $n \geqslant 1$ zbiór $A_1 \oplus \ldots \oplus A_n$ zawiera dokładnie te elementy, które należą do nieparzystej liczby zbiorów spośród $A_1, \ldots, A_n$.

3. Udowodnić następujące własności różnicy symetrycznej:

$$\bigcup_{i \in I} A_i \oplus \bigcup_{i \in I} B_i \subseteq \bigcup_{i \in I} (A_i \oplus B_i),$$

$$\bigcap_{i \in I} A_i \oplus \bigcap_{i \in I} B_i \subseteq \bigcup_{i \in I} (A_i \oplus B_i).$$

4. Udowodnić, że

$$\bigcup_{i \in I} A_i \cap \bigcup_{j \in J} B_j = \bigcup_{\langle i,j \rangle \in I \times J} (A_i \cap B_j),$$

$$\mathop{\times}_{i \in I} A_i \cap \mathop{\times}_{j \in I} B_j = \mathop{\times}_{i \in I} (A_i \cap B_i).$$

5. Niech $f\colon X \to Y$. Udowodnić, że dla dowolnych indeksowanych rodzin $\langle A_i \rangle_{i \in I}$, $\langle B_i \rangle_{i \in I}$ podzbiorów odpowiednio X i Y

$$f\Big(\bigcup_{i \in I} A_i\Big) = \bigcup_{i \in I} f(A_i),$$

$$f^{-1}\Big(\bigcup_{i \in I} B_i\Big) = \bigcup_{i \in I} f^{-1}(B_i),$$

$$f\Big(\bigcap_{i \in I} A_i\Big) \subseteq \bigcap_{i \in I} f(A_i),$$

$$f^{-1}\Big(\bigcap_{i \in I} B_i\Big) = \bigcap_{i \in I} f^{-1}(B_i).$$

Wykazać, że jeśli funkcja f jest różnowartościowa, to również w trzecim ze wzorów zachodzi równość.

6. Niech $\langle A_i \rangle_{i \in I}$ będzie indeksowaną rodziną zbiorów, z których co najmniej jeden jest skończony. Udowodnić, że $\bigcap_{i \in I} A_i \neq \emptyset$ wtedy i tylko wtedy, gdy $\bigcap_{j \in J} A_j \neq \emptyset$ dla każdego $J \subseteq_{\text{fin}} I$. Wykazać, że warunek skończoności jednego ze zbiorów jest istotny.

7 (Tarski [1]). Udowodnić, że każde odwzorowanie $F\colon \mathscr{P}(X) \to \mathscr{P}(X)$ takie, że dla dowolnych A, $B \subseteq X$

$$A \subseteq B \Rightarrow F(A) \subseteq F(B),$$

ma punkt stały, tzn. istnieje $C \subseteq X$ takie, że $F(C) = C$.

Wskazówka: $C = \bigcup \{A \in \mathscr{P}(X)\colon A \subseteq F(A)\}$.

8 (Banach [1]). Udowodnić, że dla dowolnych odwzorowań $f\colon X \to Y$ oraz $g\colon Y \to X$ istnieją zbiory X_1, X_2, Y_1, Y_2 takie, że $X = X_1 \dot\cup X_2$, $Y = Y_1 \dot\cup Y_2$, $f(X_1) = Y_1$, $g(Y_2) = X_2$.

Wskazówka: Zastosować wynik z poprzedniego zadania dla odwzorowania $F\colon \mathscr{P}(X) \to \mathscr{P}(X)$ określonego przez $F(A) = X \setminus g(Y \setminus f(X))$.

9 (Twierdzenie Cantora–Bernsteina). Udowodnić, że jeśli istnieją odwzorowania różnowartościowe $f\colon X \to Y$, $g\colon Y \to X$, to istnieje odwzorowanie wzajemnie jednoznaczne zbioru X na zbiór Y.

Wskazówka: Skorzystać z wyniku poprzedniego zadania.

10. Znaleźć wszystkie nieizomorficzne grafy niezorientowane o czterech wierzchołkach oraz wszystkie nieizomorficzne grafy zorientowane o czterech wierzchołkach.

11. Udowodnić, że jeśli $x_0, \ldots, x_n$ jest dowolną drogą w grafie (zorientowanym lub niezorientowanym), to pewien podciąg tego ciągu określa drogę elementarną z x_0 do x_n.

12. *Stopień* $d(v)$ wierzchołka v grafu $G = \langle V, E \rangle$ definiujemy jako liczbę krawędzi $e \in E$ incydentnych z v. Udowodnić, że $\sum_{v \in V} d(v) = 2|E|$.

13. Udowodnić, że dla dowolnych liczb rzeczywistych x, y

(a) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor$,
(b) $\lceil x + y \rceil \leqslant \lceil x \rceil + \lceil y \rceil$,
(c) $\lfloor -x \rfloor = -\lceil x \rceil$,
(d) $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$ $(x \geqslant 0)$,
(e) $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$ $(x \geqslant 0)$,
(f) $\lfloor \lfloor x \rfloor / n \rfloor = \lfloor x/n \rfloor$ $(n \in \boldsymbol{N})$,
(g) $\lceil \lceil x \rceil / n \rceil = \lceil x/n \rceil$ $(n \in \boldsymbol{N})$,
(h) $\sum_{i=1}^{n} \lfloor i/2 \rfloor = \lfloor n^2/4 \rfloor$,
(i) $\sum_{i=1}^{n} \lceil i/2 \rceil = \lceil n(n+2)/4 \rceil$,

14 (R. J. McEliece). Niech funkcja silnie rosnąca i ciągła $f\colon D \to \boldsymbol{R}$ będzie określona na odcinku $D \subseteq \boldsymbol{R}$ postaci $[a, b)$, $(-\infty, b]$, $[a, \infty)$ lub $\boldsymbol{R}$, gdzie a, $b \in \boldsymbol{Z}$. Wtedy następujące trzy warunki są równoważne:

(a) $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ dla każdego $x \in D$.
(b) $\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil$ dla każdego $x \in D$.
(c) Dla każdego $x \in D$, jeśli $f(x)$ jest całkowite, to x jest całkowite.

15. Wyznaczyć wszystkie nieizomorficzne porządki częściowe na zbiorze czteroelementowym.

16. Udowodnić, że przecięcie dowolnej rodziny porządków częściowych na zbiorze X jest porządkiem częściowym na zbiorze X.

17. Relację binarną $R \subseteq X \times X$ nazywamy *preporządkiem*, jeśli jest ona zwrotna i przechodnia. Określmy

$$x \approx y \Leftrightarrow x \, R \, y \wedge y \, R \, x.$$

Wykazać, że $\approx$ jest relacją równoważności na zbiorze X, oraz że wzór

$$[x]_{\approx} \leqslant [y]_{\approx} \Leftrightarrow x \, R \, y$$

definiuje (zbadać poprawność definicji!) relację porządku częściowego na $X/\approx$.

18. Udowodnić, że jeśli w zbiorze częściowo uporządkowanym skończonym istnieje dokładnie jeden element maksymalny, to jest on największym elementem zbioru. Czy założenie skończoności jest istotne?

19. Podać przykład zbioru częściowo uporządkowanego, w którym nie jest spełniony warunek (2.1). Wykazać, że w zbiorze o skończonej randze każdego elementu spełnienie tego warunku dla wszystkich x, y jest równoważne warunkowi Jordana–Dedekinda.

20. Udowodnić, że każdy porządek częściowy skończony jest izomorficzny z porządkiem postaci $\langle A, | \rangle$, gdzie $A \subseteq N$.

21. Czy w zbiorze częściowo uporządkowanym niepustym łańcuch maksymalny musi mieć niepuste przecięcie z antyłańcuchem maksymalnym?

22. Czy zbiór kół na płaszczyźnie o dowolnym środku i dowolnym promieniu uporządkowany przez zawieranie tworzy kratę?

23. Udowodnić, że w dowolnej kracie warunki

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z) \quad \text{dla wszelkich } x, y, z$$

oraz

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z) \quad \text{dla wszelkich } x, y, z$$

są równoważne.

24. Sprawdzić, że $\langle N, | \rangle$ jest kratą rozdzielną.

25. Udowodnić, że porządek częściowy $\langle X, \leqslant \rangle$ jest ufundowany wtedy i tylko wtedy, gdy każdy łańcuch $L \subseteq X$ jest dobrze uporządkowany.

26. Udowodnić, że jeśli $\langle X, \leqslant \rangle$ i porządek dualny $\langle X, \leqslant^* \rangle$ są porządkami dobrymi, to zbiór X jest skończony.

27. Udowodnić, żé suma prosta dowolnej rodziny ufundowanych porządków częściowych z zerem jest ufundowana.

28. Niech $\langle X, \leqslant \rangle$ będzie porządkiem dobrym ($|X| > 1$). Określmy na zbiorze $X^* = \bigcup_{i=1}^{\infty} X^i$ relację $\leqslant$ następująco:

$$\langle x_1, \ldots, x_n \rangle \leqslant \langle y_1, \ldots, y_m \rangle \Leftrightarrow \text{istnieje } k \leqslant n, m \text{ takie, że } x_i = y_i \text{ dla } 1 \leqslant i < k$$
$$\text{oraz } x_k < y_k, \text{ lub też } n \leqslant m \text{ i } x_i = y_i \text{ dla } 1 \leqslant i \leqslant n.$$

Czy ta relacja dobrze porządkuje zbiór X^*?

29. Udowodnić zmodyfikowaną wersję twierdzenia 2.5, w której $h\colon \mathscr{P} \times X \to Y$, i definicja indukcyjna ma postać $f(x) = h(f \upharpoonright B_x, x)$ (funkcja f określona przez tę definicję może przyjmować różne wartości dla różnych elementów minimalnych).

30. Udowodnić, że liczba sposobów, którymi można rozsadzić n spośród m osób przy okrągłym stole, jest równa $[m]_n/n$ (utożsamiamy rozsadzenia różniące się jedynie cyklicznym przesunięciem osób wokół stołu).

31. W turnieju pięściarskim uczestniczy 16 zawodników. Ile jest możliwych sposobów rozdzielenia medali: złotego, srebrnego i dwóch równorzędnych brązowych? (Zakładamy, że rozstawienie zawodników nie jest ustalone, lecz wybrane losowo na początku turnieju.) Ile jest możliwych sposobów rozdzielenia medali dla każdego ustalonego rozstawienia zawodników? (Turniej rozgrywany jest systemem: $\frac{1}{8}$ finału, ćwierćfinały, półfinały i finał.)

32. Ile spośród liczb pomiędzy 1000 i 10000 składa się z cyfr nieparzystych, a ile z cyfr różnych?

33. Ile jest możliwych rezultatów, którymi mogą się zakończyć zawody, w których startuje 8 osób w trzech konkurencjach, jeśli każda osoba startuje w jednej, dowolnie przez siebie wybranej konkurencji? (Przez rezultat zawodów rozumiemy zestawienie kolejności wszystkich zawodników startujących w każdej z konkurencji; nie zakładamy, że każda konkurencja jest obsadzona przez co najmniej jedną osobę.)

34. Ile palindromów długości n można utworzyć używając m liter alfabetu? (*Palindromem* nazywamy dowolne słowo, które brzmi tak samo czytane w przód, jak i wspak, na przykład

Ada, panna, pocałowana woła: Co pan napada?!

– po pominięciu spacji, znaków interpunkcyjnych, oraz utożsamieniu małych i dużych liter.)

35. *Inwersją* permutacji $f \in S_n$ nazywamy dowolną parę $\langle i, j \rangle$ taką, że $1 \leqslant i < j \leqslant n$ oraz $f(i) > f(j)$. Znak permutacji określamy następująco:

$$\operatorname{sgn}(f) = (-1)^{I(f)},$$

gdzie $I(f)$ jest liczbą inwersji permutacji f. Permutację f nazywamy *parzystą*, jeśli $\operatorname{sgn}(f) = 1$, oraz *nieparzystą*, jeśli $\operatorname{sgn}(f) = -1$. Udowodnić, że

(a) Każdą permutację można przedstawić w postaci złożenia $I(f)$ transpozycji sąsiednich elementów, tzn. permutacji postaci pojedynczego cyklu $[i\ i+1]$, $1 \leqslant i < n$.

(b) $\operatorname{sgn}(fg) = \operatorname{sgn}(f)\operatorname{sgn}(g)$ dla dowolnych $f, g \in S_n$.

(c) Zbiór A_n permutacji parzystych zbioru $\{1, \ldots, n\}$ tworzy grupę względem składania permutacji, przy czym dla $n > 1$ mamy $|A_n| = |S_n|/2 = n!/2$.

(d) Jeśli f jest cyklem długości k, to $\operatorname{sgn}(f) = (-1)^{k-1}$.

(e) Znak permutacji f typu $1^{\lambda_1} 2^{\lambda_2} \ldots n^{\lambda_n}$ wyraża się wzorem

$$\operatorname{sgn}(f) = (-1)^{\lambda_2 + \lambda_4 + \ldots}.$$

(Wzór ten pozwala mówić o znaku permutacji dowolnego zbioru skończonego X – niekoniecznie $X = \{1, \ldots, n\}$ – mimo iż w takim przypadku traci sens pojęcie inwersji.)

36. *Inwolucją* nazywamy dowolną permutację f taką, że ff jest permutacją identycznościową. Udowodnić, że $f \in S_n$ jest inwolucją wtedy i tylko wtedy, gdy jest typu $1^{\lambda_1} 2^{\lambda_2}$, $\lambda_1 + 2\lambda_2 = n$, oraz że dowolna permutacja jest złożeniem dwóch inwolucji.

37. Dla permutacji $\langle f_1, \ldots, f_n \rangle$ zbioru $\{1, \ldots, n\}$ definiujemy *wektor inwersyjny* jako $\langle d_1, \ldots, d_n \rangle$, gdzie

$$d_i = |\{j\colon j < i \wedge a_j > a_i\}|.$$

Udowodnić, że każdy ciąg $\langle d_1, \ldots, d_n \rangle$, gdzie $0 \leqslant d_i \leqslant i-1$, jest wektorem inwersyjnym dokładnie jednej permutacji.

38. Udowodnić, że wszystkie $n!$ permutacji zbioru $\{1, \ldots, n\}$, $n > 1$, można ustawić w ciąg cykliczny tak, że każdą następną permutację można otrzymać z poprzedniej przez złożenie z pewną transpozycją elementów sąsiednich.

39. Będziemy mówili, że element f_i stanowi dla permutacji $\langle f_1, \ldots, f_n \rangle \in S_n$ minimum lokalne, jeśli $f_j > f_i$ dla wszelkich $j < i$ (f_1 jest zawsze minimum lokalnym). Udowodnić, że liczba permutacji $f \in S_n$ o dokładnie k minimach lokalnych jest równa $|s(n, k)|$.

Wskazówka: Każdej permutacji o k cyklach odpowiada jednoznacznie permutacja o k minimach lokalnych, otrzymana przez zapisanie każdego cyklu poczynając od jego najmniejszego elementu, a następnie przez ustawienie cykli w kolejności malejących elementów minimalnych.

40. Udowodnić, że średnia liczba cykli dla losowo wybranej permutacji zbioru n-elementowego wynosi

$$\sum_{k=1}^{n} \frac{1}{k},$$

tzn.

$$\frac{1}{n!}\sum_{k=1}^{n}|s(n,k)|\,k=\sum_{k=1}^{n}\frac{1}{k}.$$

41. Dla każdej permutacji $f=\langle f_1,\ldots,f_n\rangle$ zbioru $\{1,\ldots,n\}$ niech $\alpha(f)=|\{i\colon 1\leqslant i<n \wedge f_i>f_{i+1}\}|+1$, tzn. $\alpha(f)$ jest liczbą odcinków rosnących, z jakich składa się $\langle f_1,\ldots,f_n\rangle$. *Liczby Eulera* $A_{n,k}$ definijemy następująco:

$$A_{n,k}=|\{f\in S_n\colon \alpha(f)=k\}|.$$

Udowodnić, że

(a) $A_{n,k}=0$ dla $k>n>1$, $A_{n,0}=0$, $A_{0,1}=1$,
$A_{n,k}=kA_{n-1,k}+(n-k+1)A_{n-1,k-1}$ dla $n\geqslant 1$,

(b) $\sum_{k=0}^{n}A_{n,k}=n!$,

(c) $A_{n,k}=A_{n,n+1-k}$ $(n\geqslant 1)$,

(d) $\sum_{k=0}^{n}A_{n,k}\binom{m+k-1}{n}=m^n$ $(n\geqslant 0)$,

(e) $x^n=\sum_{k=1}^{n}A_{n,k}\binom{x+k-1}{n}$,

(f) $A_{n,k}=\sum_{i=0}^{k}(-1)^i(k-i)^n\binom{n+1}{i}$ $(n,k\geqslant 0)$,

(g) $\sum_{k=1}^{n}A_{n,k}\binom{k-1}{n-m}=m!\,S(n,m)$.

42 (Lipski i Preparata [1]). Udowodnić, że dla każdego n zbiór wszystkich permutacji zbioru $\{1,\ldots,n\}$ można ustawić w ciąg $f_1,f_2,\ldots,f_{n!}$ o tej własności, że dla każdego $i\in\{1,\ldots,n\}$ ciąg $f_1(i),f_2(i),\ldots,f_{n!}(i)$ jest taki sam z dokładnością do cyklicznego przesuniecia.

43. Oznaczając $[x]^n=x(x+1)\ldots(x+n-1)$ wykazać, że

$$[x]^n=\sum_{k=0}^{n}|s(n,k)|\,x^k.$$

44. Udowodnić, że dla dowolnych $p,q,n\in N_0$

$$[p+q]_n=\sum_{k=0}^{n}\binom{n}{k}[p]_k[q]_{n-k},$$

$$[p+q]^n=\sum_{k=0}^{n}\binom{n}{k}[p]^k[q]^{n-k}.$$

Wskazówka: W przypadku pierwszej tożsamości obliczyć na dwa sposoby liczbę wszystkich funkcji różnowartościowych $f\colon X\to Y$, gdzie $|X|=n$, $Y=P\mathbin{\dot\cup}Q$, $|P|=p$, $|Q|=q$. Dla drugiej tożsamości znaleźć podobną interpretację w terminach rozmieszczeń uporządkowanych w $p+q$ pudełkach.

45. Udowodnić, że liczba $f(n,k)$ podzbiorów k-elementowych zbioru $\{1,\ldots,n\}$ nie zawierających żadnej pary kolejnych liczb jest równa

$$f(n,k)=\binom{n-k+1}{k}.$$

Wskazówka: $\langle a_1,\ldots,a_k\rangle$ jest ciągiem elementów zbioru $\{1,\ldots,n\}$ spełniających warunek $a_{i+1}>a_i+1$, $1\leqslant i<k$, wtedy i tylko wtedy, gdy $a_1,a_2-1,\ldots,a_k-k+1$ jest ciągiem rosnącym elementów zbioru $\{1,\ldots,n-k+1\}$.

46. Udowodnić, że zbiory rodziny $\mathscr{P}_k(X)$, gdzie $0 < k < |X|$, można ustawić w ciąg cykliczny taki, że każdy następny podzbiór powstaje z poprzedniego przez usunięcie pewnego elementu i dodanie innego. Udowodnić, że zbiory rodziny $\mathscr{P}(X)$ można ustawić w ciąg cykliczny taki, że każdy następny podzbiór powstaje z poprzedniego przez usunięcie lub dodanie pewnego elementu.

47. Udowodnić, że

$$\binom{n}{0} < \binom{n}{1} < \ldots < \binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil} > \ldots > \binom{n}{n}.$$

48. Udowodnić, że iloczyn dowolnych kolejnych k liczb naturalnych jest podzielny przez $k!$.

Wskazówka: Rozważyć współczynnik dwumienny $\binom{n+k}{n}$.

49. Udowodnić następujące tożsamości:

(a) $\sum_{k=1}^{n} k^2 \binom{n}{k} = n(n+1)2^{n-2}$,

(b) $\sum_{k=0}^{n} (-1)^k \binom{n}{k}\binom{k}{j} = \begin{cases} 0, & \text{jeśli } n \neq j, \\ (-1)^n, & \text{jeśli } n = j, \end{cases}$

(c) $\sum_{k=1}^{n} \frac{(-1)^{k+1}}{k}\binom{n}{k} = \sum_{k=1}^{n} \frac{1}{k}$,

(d) $\sum_{k=0}^{n} (-1)^k \binom{x}{n-k}\binom{y+k}{k} = \binom{x-y-1}{n}$,

(e) $\sum_{k=0}^{n} (-1)^k \binom{x}{k} = \binom{n-x}{n} = (-1)^n \binom{x-1}{n} = \prod_{k=1}^{n}\left(1-\frac{x}{k}\right)$,

(f) $\sum_{i=0}^{k} (-1)^i \binom{k}{i}\binom{n+i}{l} = (-1)^k \binom{n}{l-k}$,

(g) $\sum_{k=0}^{n} (-1)^k \frac{\binom{n}{k}\binom{x}{k}}{\binom{y}{k}} = \frac{\binom{y-x}{n}}{\binom{y}{n}}$,

(h) $\sum_{k=0}^{n} (-1)^k \frac{\binom{n}{k}}{\binom{x+k}{k}} = \frac{x}{x+n}$,

(i) $\sum_{k=0}^{p} \binom{p}{k}\binom{q}{k} x^{p-k} y^k = \sum_{k=0}^{p} \binom{p}{k}\binom{q+k}{k}(x-y)^{p-k} y^k$.

50. Ile liczb naturalnych nie przekraczających 1000 nie dzieli się przez 3, 7 ani przez 11?

51. Iloma sposobami można na szachownicy wymiaru 8×8 rozmieścić 8 wież tak, by żadne dwie nie atakowały się wzajemnie i żadna z nich nie była umieszczona na wybranej przekątnej szachownicy.

52. Znaleźć liczbę ciągów długości $2n$ takich, że każda liczba $i \in \{1, \ldots, n\}$ występuje dokładnie dwa razy, przy czym żadne dwa kolejne wyrazy nie są równe.

Wskazówka: Zastosować zasadę włączania–wyłączania.

53. Stosując zasadę włączania–wyłączania znaleźć liczbę podzbiorów 11-elementowych zbioru z powtórzeniami $(4*a,\ 3*b,\ 7*c)$.

54. Udowodnić, że

$$|P_1 \oplus \ldots \oplus P_k| = W(1) - 2W(2) + 4W(3) - 8W(4) + \ldots + (-2)^{k-1} W(k),$$

gdzie $W(i)$ jest określone wzorem (7.2).

55. Udowodnić następujące zależności dotyczące liczby D_n nieporządków na zbiorze n-elementowym:

$$D_{n+1} = (n+1)D_n + (-1)^{n+1},$$

$$D_{n+1} = n(D_n + D_{n-1}).$$

56. Podać przykład pokazujący, iż krata $\Pi(X)$ nie jest rozdzielna dla $|X| \geqslant 3$.

57. Udowodnić, że $|\pi \vee \sigma| + |\pi \wedge \sigma| \geqslant |\pi| + |\sigma|$ dla dowolnych $\pi, \sigma \in \Pi(X)$.

58. Udowodnić, że wszystkie podziały ustalonego zbioru X można ustawić w ciąg taki, że każdy następny podział powstaje z poprzedniego przez usunięcie elementu z pewnego bloku podziału (jeśli ten blok był jednoelementowy, to ulega on likwidacji) i albo przeniesienie go do innego bloku podziału, albo też utworzenie z niego nowego bloku jednoelementowego.

59. Niech $M(n)$ oznacza tę wartość k, dla której wartość liczby Stirlinga $S(n, k)$ jest największa (dokładniej, największa z liczb k o tej własności). Udowodnić, że albo

$$S(n, 0) < S(n, 1) < \ldots < S(n, M(n)) > S(n, M(n)+1) > \ldots > S(n, n),$$

albo też

$$S(n, 0) < S(n, 1) < \ldots < S(n, M(n)-1) = S(n, M(n)) > \ldots > S(n, n).$$

Wykazać ponadto, że $0 \leqslant M(n-1) - M(n) \leqslant 1$.

60. Udowodnić, że

(a) $\binom{i+j}{i} s(n, i+j) = \sum_{k=0}^{n} \binom{n}{k} s(k, i)\, s(n-k, j)$,

(b) $\binom{i+j}{i} S(n, i+j) = \sum_{k=0}^{n} \binom{n}{k} S(k, i)\, S(n-k, j)$.

61. Udowodnić wzory

(a) $|s(n, k)| = \sum_{0 < m_1 < m_2 < \ldots < m_{n-k} < n} m_1 m_2 \ldots m_{n-k}$,

(b) $S(n, k) = \sum_{0 \leqslant m_1 \leqslant m_2 \leqslant \ldots \leqslant m_{n-k} \leqslant k} m_1 m_2 \ldots m_{n-k}$.

62. Oznaczmy dla każdego $k \geqslant 0$

$$g^{(k)} = \frac{d^k}{dx^k} g(x), \qquad f^{(k)} = \frac{d^k}{dy^k} f(y)\bigg|_{y=g(x)}.$$

Udowodnić, że n-ta pochodna złożenia $f(g(x))$ wyraża się następującym *wzorem Faa di Bruno*:.

$$\frac{d^n}{dx^n} f(g(x)) = \sum_{j=0}^{n} \sum_{\substack{k_1+k_2+\ldots+k_n=j \\ k_1+2k_2+\ldots+nk_n=n \\ k_1, k_2, \ldots, k_n \geqslant 0}} f^{(j)} \frac{n!\,(g^{(1)})^{k_1} \ldots (g^{(n)})^{k_n}}{k_1!\,(1!)^{k_1} \ldots k_n!\,(n!)^{k_n}}.$$

Wykazać, że jeśli to wyrażenie będziemy traktowali jako wielomian zmiennych $f^{(i)}, g^{(i)}, i = 1, \ldots, n$, to suma współczynników tego wielomianu jest równa liczbie Bella B_n.

63. Rodzinę $\mathfrak{M}$ podzbiorów zbioru skończonego X nazywamy *zrównoważoną*, jeśli dla wszelkich $\mathfrak{N}_1, \mathfrak{N}_2 \subseteq \mathfrak{M}$

$$|\mathfrak{N}_1| = |\mathfrak{N}_2| \Rightarrow \left|\bigcap \mathfrak{N}_1\right| = \left|\bigcap \mathfrak{N}_2\right|.$$

Udowodnić, że rodzina $\mathfrak{M} = \{M_1, \ldots, M_n\}$ podzbiorów zbioru X jest zrównoważona wtedy i tylko

wtedy, gdy jej składowe spełniają, dla wszelkich ε, $\varepsilon' \in \{0, 1\}^n$, warunek

$$|\varepsilon| = |\varepsilon'| \Rightarrow |S(\varepsilon)| = |S(\varepsilon')|,$$

gdzie $|\varepsilon| = \varepsilon_1 + \ldots + \varepsilon_n$.

64. Udowodnić następujące własności liczb Fibonacciego:

(a) $f_{n+m} = f_n f_m + f_{n-1} f_{m-1}$,

(b) $(f_n, f_m) = f_{(n+1, m+1)-1}$, $m, n > 1$,

gdzie (a, b) oznacza największy wspólny dzielnik liczb a, b,

(c) $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^{n+1} = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$, $n \geqslant 0$

(przyjmujemy $f_{-1} = 0$, podobnie w następującym punkcie),

(d) $f_n^2 - f_{n+1} f_{n-1} = (-1)^n$,

(e) $f_{n+1} = \sum_{k=0}^{\lfloor (n+1)/2 \rfloor} \binom{n-k+1}{k}$,

(f) $f_n = 2^{-n} \sum_{k=0}^{\lceil n/2 \rceil} \binom{n+1}{2k+1} 5^k$.

65. Udowodnić, że liczba sposobów, w jakie można szachownicę wymiaru $n \times 2$ pokryć „kostkami domino" (wymiaru 2×1), jest równa liczbie Fibonacciego f_n.

66. Opisać metodę rozwiązywania równań rekurencyjnych postaci

$$a_n = A_1 a_{n-1} + A_2 a_{n-2} + \ldots + A_k a_{n-k}$$

(z warunkami początkowymi określającymi wartości $a_1, \ldots, a_k$) za pomocą funkcji tworzących, analogiczną do metody użytej przy wyznaczaniu liczb Fibonacciego.

67. Niech a_n będzie liczbą ciągów różnowartościowych o elementach ze zbioru n-elementowego, tzn. $a_n = \sum_{k=0}^{n} [n]_k$. Udowodnić, że

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = \frac{e^x}{1-x}.$$

68. Niech a_n będzie liczbą inwolucji w S_n (por. zad. 36). Udowodnić, że

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n = e^{x+(x^2/2)}.$$

69. Udowodnić, że liczba podziałów uporządkowanych liczby n na k składników (tzn. liczba ciągów $\langle b_1, \ldots, b_k \rangle$ takich, że $b_1, \ldots, b_k > 0$ oraz $b_1 + \ldots + b_k = n$) jest równa $\binom{n-1}{k-1}$, oraz że liczba wszystkich podziałów uporządkowanych liczby n na dowolną liczbę składników jest równa 2^{n-1}.

70. Udowodnić, że liczbę podziałów liczby n na k składników można przedstawić w postaci

$$P(n, k) = \frac{n^{k-1}}{(k-1)!\,k!} + R_{k-2}(n),$$

gdzie $R_{k-2}(n)$ jest pewnym wielomianem zmiennej n stopnia co najwyżej $k-2$, którego współczynniki zależą od reszty $n \bmod k!$ (tzn. dla ustalonego k możemy zdefiniować $P(n, k)$ przez $k!$ wielomianów

zmiennej n stopnia $k-1$). Wykazać w szczególności, że

$$P(n, 2) = \begin{cases} \frac{n}{2}, & \text{jeśli } n \equiv 0 \pmod 2, \\ \frac{n-1}{2}, & \text{jeśli } n \equiv 1 \pmod 2, \end{cases}$$

$$P(n, 3) = \begin{cases} \frac{n^2}{12}, & \text{jeśli } n \equiv 0 \pmod 6, \\ \frac{n^2}{12} - \frac{1}{12}, & \text{jeśli } n \equiv 1 \pmod 6, \\ \frac{n^2}{12} - \frac{1}{3}, & \text{jeśli } n \equiv 2 \pmod 6, \\ \frac{n^2}{12} + \frac{1}{4}, & \text{jeśli } n \equiv 3 \pmod 6, \\ \frac{n^2}{12} - \frac{1}{3}, & \text{jeśli } n \equiv 4 \pmod 6, \\ \frac{n^2}{12} - \frac{1}{12}, & \text{jeśli } n \equiv 5 \pmod 6 \end{cases}$$

(tzn. $P(n, 2) = \lfloor n/2 \rfloor$, $P(n, 3)$ zaś jest liczbą całkowitą najbliższą $n^2/12$).

Znaleźć analogiczny wzór dla $P(n, 4)$.

71. Udowodnić, że

$$\sum_{n=0}^{\infty} P(n) x^n = \prod_{i=1}^{\infty} (1-x^i)^{-1},$$

przy czym iloczyn po prawej stronie jest zbieżny jednostajnie w pewnym otoczeniu zera.

72. Korzystając z twierdzenia Eulera (twierdzenie 11.5) udowodnić następującą *tożsamość Eulera*:

$$\prod_{i=1}^{\infty} (1-x^i) = 1 + \sum_{k=1}^{\infty} (-1)^k (x^{(3k^2-k)/2} + x^{(3k^2+k)/2})$$

(zbadać zbieżność iloczynu po lewej i szeregu po prawej stronie).

73. Uzupełnić brakujące fragmenty dowodu faktu, iż krata $\mathscr{L}(n, q)$ jest samodualna (p. § 12).

74. Udowodnić, że

$$\binom{n}{0}_q < \binom{n}{1}_q < \ldots < \binom{n}{\lfloor n/2 \rfloor}_q = \binom{n}{\lceil n/2 \rceil}_q > \ldots > \binom{n}{n}_q.$$

75. Niech a_i będzie liczbą podziałów liczby i na co najwyżej k części, z których żadna nie przekracza $n-k$. Udowodnić, że

$$\sum_{i=0}^{\infty} a_i q^i = \binom{n}{k}_q$$

(q jest potęgą liczby pierwszej).

76. Udowodnić, że warstwa przestrzeni liniowej nad ciałem K rozpięta przez podzbiór A tej przestrzeni jest zbiorem wszystkich elementów postaci $\lambda_1 a_1 + \ldots + \lambda_m a_m$, gdzie $m \geqslant 1$, $\lambda_1, \ldots, \lambda_m \in K$, $\lambda_1 + \ldots + \lambda_m = 1$ oraz $a_1, \ldots, a_m \in A$.

77. Udowodnić, że podzbiór A zbioru punktów geometrii $AG(n, q)$ jest podprzestrzenią tej

geometrii wtedy i tylko wtedy, gdy dla każdych dwóch różnych punktów a, $b \in A$ prosta przechodząca przez te punkty jest zawarta w A.

78. *Geometrią rzutową* nazywamy każdą parę $\langle X, \mathscr{B}\rangle$, gdzie X jest zbiorem, którego elementy nazywamy *punktami*, $\mathscr{B}$ zaś pewną rodziną jego podzbiorów, zwanych *prostymi*, oraz spełnione są warunki:

GR1. Przez każde dwa różne punkty przechodzi dokładnie jedna prosta.

GR2. Dla każdych punktów a, b, c nie leżących na jednej prostej, oraz każdych punktów d, e różnych od a i takich, że zarówno a, b, d jak i a, c, e leżą na jednej prostej, proste przechodzące odpowiednio przez b, c oraz d, e przecinają się.

GR3. Każda prosta zawiera co najmniej trzy różne punkty.

Udowodnić, że w każdej geometrii rzutowej wszystkie proste są tej samej liczności, oraz że przez każdy punkt przechodzi ta sama liczba prostych. Wykazać, że warunki GR1, GR2, GR3 są spełnione w każdej geometrii $PG(n, q)$.

79. W każdej geometrii rzutowej $\langle X, \mathscr{B}\rangle$ (p. poprzednie zadanie) definiujemy indukcyjnie podprzestrzeń wymiaru n w następujący sposób. Przez podprzestrzeń wymiaru 0 rozumiemy każdy punkt geometrii. Podzbiór $A \subseteq X$ jest podprzestrzenią wymiaru n, jeśli istnieje podprzestrzeń B wymiaru $n-1$ oraz punkt $p \in X \setminus B$ taki, że $A = \bigcup_{b \in B} L_{pb}$, gdzie L_{pb} oznacza prostą przechodzącą przez punkty p i b.

Udowodnić, że ta definicja jest poprawna, tzn. że niemożliwa jest sytuacja, w której $\bigcup_{b \in B} L_{pb} = \bigcup_{c \in C} L_{sc}$, przy czym $b \in X \setminus B$, $s \in X \setminus C$ oraz B i C są podprzestrzeniami różnego wymiaru). Wykazać, że w przypadku geometrii $PG(n, q)$ wymiar określony przez tę definicję pokrywa się z wymiarem zdefiniowanym dla geometrii $PG(n, q)$ w § 12.

80. Udowodnić, że podprzestrzenie każdej geometrii rzutowej (z dołączonym zbiorem pustym, traktowanym jako podprzestrzeń wymiaru -1) uporządkowane częściowo przez zawieranie tworzą kratę, w której

$$A \supseteq B \Rightarrow A \wedge (B \vee C) = B \vee (A \wedge C),$$

dla dowolnych podprzestrzeni A, B, C. Udowodnić, że

$$\dim(A \vee B) + \dim(A \wedge B) = \dim A + \dim B,$$

gdzie dim oznacza wymiar określony w poprzednim zadaniu.

81. Udowodnić, że każda geometria rzutowa wymiaru 2 (p. zad. 78 i 79) jest płaszczyzną rzutową, tzn. spełnia warunki PR1, PR2, PR3.

82. Udowodnić, że opisana w § 12 konstrukcja płaszczyzny rzutowej z płaszczyzny afinicznej zastosowana do $AG(2, q)$ daje płaszczyznę izomorficzną z $PG(2, q)$. Wykazać, że opisana tam konstrukcja odwrotna zastosowana do płaszczyzny $PG(2, q)$ daje płaszczyznę izomorficzną z $AG(2, q)$ niezależnie od wyboru „prostej w nieskończoności".

83. Udowodnić, że jedyną, z dokładnością do izomorfizmu, płaszczyzną rzutową rzędu 2 jest $PG(2,2)$.

ALGEBRA INCYDENCJI I TWIERDZENIA INWERSYJNE W ZBIORACH CZĘŚCIOWO UPORZĄDKOWANYCH

W niniejszym rozdziale zajmiemy się uogólnieniem oczywistej zależności

$$G(i) = \sum_{j:j \leqslant i} F(j) \Leftrightarrow F(i) = G(i) - G(j-1)$$

(o funkcji F zakładamy, że jest określona dla dowolnych liczb całkowitych, oraz $F(j) = 0$ dla j mniejszych od pewnej liczby). Zamiast zbioru liczb całkowitych, uporządkowanego przez relację $\leqslant$, możemy mianowicie rozważać dowolny lokalnie skończony zbiór częściowo uporządkowany. Określmy dla każdego elementu x takiego zbioru

$$G(x) = \sum_{y:y \leqslant x} F(y),$$

gdzie o funkcji F zakładamy, że dla każdego x suma po prawej stronie zawiera jedynie skończoną liczbę składników różnych od zera. Powstaje naturalne pytanie: w jaki sposób wyznaczyć funkcję F mając daną funkcję G? Odpowiedź na to pytanie, jak się przekonamy, jest dana przez wzór inwersyjny Möbiusa postaci

$$F(x) = \sum_{y:y \leqslant x} G(y)\,\mu(y, x),$$

gdzie μ jest pewną funkcją, zwaną funkcją Möbiusa, zależną jedynie od struktury rozważanego zbioru częściowo uporządkowanego. W rozdziale tym wyznaczymy funkcję Möbiusa dla wielu zbiorów częściowo uporządkowanych i pokażemy zastosowania otrzymanych w ten sposób wzorów inwersyjnych.

§ 1. Algebra incydencji

Przypomnijmy, że zbiór częściowo uporządkowany $\boldsymbol{P} = \langle P, \leqslant \rangle$ nazywamy *lokalnie skończonym*, jeśli odcinek $[x, y]$ jest skończony dla dowolnych $x, y \in P$. *Algebra incydencji* $\mathscr{A}(\boldsymbol{P})$ lokalnie skończonego zbioru częściowo uporządko-

wanego $\boldsymbol{P} = \langle P, \leqslant \rangle$ składa się z wszystkich funkcji rzeczywistych $f\colon P \times P \to \boldsymbol{R}$ spełniających warunek

(1.1) $$x \nleqslant y \Rightarrow f(x, y) = 0$$

(innymi słowy: $f(x, y) \neq 0 \Rightarrow x \leqslant y$) dla dowolnych $x, y \in P$, z działaniami *dodawania*, *mnożenia przez skalar* oraz *splotu* określonymi następująco:

$$(f+g)(x, y) = f(x, y) + g(x, y),$$

$$(cf)(x, y) = c \cdot f(x, y),$$

(1.2) $$(f * g)(x, y) = \sum_{z : x \leqslant z \leqslant y} f(x, z) g(z, y)$$

dla dowolnych f, g w $\mathscr{A}(\boldsymbol{P})$, $x, y \in P$, $c \in \boldsymbol{R}$. Jeśli $x \nleqslant y$, to sumę pustego zbioru składników po prawej stronie (1.2) interpretujemy — jak zwykle — jako zero. Definicja splotu wyjaśnia, dlaczego w naszych rozważaniach ograniczamy się do zbiorów lokalnie skończonych: gwarantuje to skończoność sumy (1.2). Zauważmy jeszcze, że jeśli w naturalny sposób zdefiniujemy sumę dowolnego zbioru liczb, z których tylko skończona ilość jest różna od zera, to splot (1.2) możemy zapisać po prostu jako $\sum_{z \in P} f(x, z) g(z, y)$. Zamiast ciała $\boldsymbol{R}$ możemy przyjąć dowolne inne ciało, a nawet pierścień przemienny z jedynką, bez istotnych zmian w teorii rozważanej w tym rozdziale.

Zdefiniujmy pewien szczególny element δ algebry $\mathscr{A}(\boldsymbol{P})$ następująco:

$$\delta(x, y) = \begin{cases} 1, & \text{jeśli } x = y, \\ 0, & \text{jeśli } x \neq y. \end{cases}$$

Wykażemy teraz, że $\mathscr{A}(\boldsymbol{P})$ jest *algebrą z jedynką*, tzn. przestrzenią liniową (nad ciałem $\boldsymbol{R}$) z dodatkowym działaniem — w naszym przypadku splotem — które jest łączne, obustronnie rozdzielne względem dodawania, ma element neutralny (jedynkę) oraz spełnia warunek $(cf) * g = f * (cg) = c(f * g)$.

TWIERDZENIE 1.1. *$\mathscr{A}(\boldsymbol{P})$ jest algebrą z jedynką δ.*

Dowód. Wykażemy najpierw łączność splotu:

$$\begin{aligned}
((f * g) * h)(x, y) &= \sum_{z : x \leqslant z \leqslant y} (f * g)(x, z) h(z, y) = \\
&= \sum_{z : x \leqslant z \leqslant y} \Big(\sum_{t : x \leqslant t \leqslant z} f(x, t) g(t, z) \Big) h(z, y) = \\
&= \sum_{z, t : x \leqslant t \leqslant z \leqslant y} f(x, t) g(t, z) h(z, y) = \\
&= \sum_{t : x \leqslant t \leqslant y} f(x, t) \Big(\sum_{z : t \leqslant z \leqslant y} g(t, z) h(z, y) \Big) = \\
&= \sum_{t : x \leqslant t \leqslant y} f(x, t) (g * h)(t, y) = (f * (g * h))(x, y).
\end{aligned}$$

Funkcja δ jest istotnie jedynką, gdyż

$$(\delta * f)(x, y) = \sum_{z: x \leqslant z \leqslant y} \delta(x, z) f(z, y) = \delta(x, x) f(x, y) = f(x, y),$$

i podobnie $f * \delta = f$. Pozostałe warunki są oczywiste, pozostawiamy je do sprawdzenia Czytelnikowi. □

Łatwo się przekonać, że działanie splotu na ogół nie jest przemienne (p. zad. 2). Zauważmy, że jeśli pominiemy działanie mnożenia przez element ciała, to $\mathscr{A}(\boldsymbol{P})$ możemy traktować jako pierścień (na ogół nieprzemienny) z jedynką. Właśnie ta struktura pierścienia okaże się najbardziej istotna w dalszym ciągu.

Element f algebry z jedynką 1 nazywamy *odwracalnym*, jeśli istnieje element g taki, że $f \cdot g = g \cdot f = 1$. Element g — jeśli istnieje — jest wyznaczony jednoznacznie przez f. Istotnie, jeśli $g' \cdot f = 1$, to

(1.3) $$g' = g' \cdot 1 = g' \cdot (f \cdot g) = (g' \cdot f) \cdot g = 1 \cdot g = g.$$

Ten jednoznacznie wyznaczony element g nazywamy *odwrotnością* elementu f i oznaczamy przez f^{-1}. Zauważmy, iż z (1.3) wynika, że jeśli g jest odwrotnością prawostronną, g' zaś odwrotnością lewostronną elementu f (tzn. $f \cdot g = 1$, $g' \cdot f = 1$), to $g = g' = f^{-1}$.

Twierdzenie 1.2. *Element f algebry incydencji $\mathscr{A}(\boldsymbol{P})$ jest odwracalny wtedy i tylko wtedy, gdy $f(x, x) \neq 0$ dla każdego $x \in P$.*

Dowód. Niech $f(x, x) \neq 0$ dla każdego $x \in P$. Udowodnimy, że element f jest odwracalny. W tym celu ustalmy dowolny element $x \in P$. Zbiór $\{y \in P\colon y \geqslant x\}$ wraz z relacją porządku dziedziczoną z $\boldsymbol{P}$ jest ufundowany (p. § 1.2), możemy zatem stosować twierdzenie o definiowaniu przez indukcję (twierdzenie 1.2.6). Przyjmujemy

(1.4) $$g(x, x) = \frac{1}{f(x, x)}$$

oraz

(1.5) $$g(x, y) = \frac{1}{f(y, y)} \Big(- \sum_{z: x \leqslant z < y} g(x, z) f(z, y)\Big)$$

przy założeniu, że wartości $g(x, z)$ zostały już określone dla wszystkich z takich, że $x \leqslant z < y$. Na mocy twierdzenia o definiowaniu przez indukcję wzory (1.4), (1.5) określają jednoznacznie $g(x, y)$ dla wszystkich $y \geqslant x$. Powtarzając tę konstrukcję dla każdego $x \in P$ oraz przyjmując $g(x, y) = 0$ dla $x \nleqslant y$ określamy pewną funkcję $g \in \mathscr{A}(\boldsymbol{P})$. Obliczmy splot $g * f$. Mamy

$$(g * f)(x, x) = g(x, x) f(x, x) = 1$$

oraz

$$(g * f)(x, y) = \sum_{z: x \leqslant z \leqslant y} g(x, z) f(z, y) = 0,$$

jeśli $x < y$ (mnożymy obie strony wzoru (1.5) przez $f(y, y)$ i przenosimy prawą stronę na lewą). Tak więc $g * f = \delta$ i g jest odwrotnością lewostronną elementu f. W podobny sposób, stosując wzory

$$g'(x, x) = \frac{1}{f(x, x)},$$

$$g'(x, y) = \frac{1}{f(x, x)}\Big(- \sum_{z:\, x < z \leqslant y} f(x, z)\, g'(z, y)\Big),$$

definiujemy odwrotność prawostronną g'. Z poprzednich rozważań wynika, że $g = g' = f^{-1}$.

Na odwrót, jeśli element f ma odwrotność lewostronną lub prawostronną, to $g(x, x) f(x, x) = 1$ (odpowiednio $f(x, x) g'(x, x) = 1$), czyli $f(x, x) \neq 0$. □

Uwaga: Jeśli rozważamy algebrę incydencji złożoną z funkcji o wartościach w pewnym pierścieniu z jedynką R, to zamiast $f(x, x) \neq 0$ musimy żądać, by $f(x, x)$ był elementem odwracalnym w tym pierścieniu. Zauważmy, że z dowodu twierdzenia 1.2 wynika, że każda odwrotność lewostronna (prawostronna) jest automatycznie odwrotnością, o ile własność ta przysługuje pierścieniowi R.

Definicja splotu wykazuje pewne podobieństwo do iloczynu $[\sum_{k=1}^{n} f_{ik} g_{kj}]$ macierzy $[f_{ij}]$, $[g_{ij}]$. Istotnie, ograniczając się do przypadku, gdy zbiór P jest skończony, powiedzmy $P = \{x_1, \ldots, x_n\}$, możemy przyporządkować każdej funkcji f macierz $M(f) = [f_{ij}]$ wymiaru $n \times n$ zdefiniowaną następująco:

$$f_{ij} = f(x_i, x_j).$$

Łatwo zauważyć, że splotowi $f * g$ odpowiada wtedy iloczyn macierzy $M(f)$, $M(g)$:

$$M(f * g) = M(f) \cdot M(g).$$

Każdy porządek częściowy można rozszerzyć do porządku liniowego, możemy zatem zakładać, że

$$x_i \leqslant x_j \Rightarrow i \leqslant j$$

dla $1 \leqslant i, j \leqslant n$. Przy takim ponumerowaniu elementów zbioru P macierz $M(f)$ odpowiadająca elementowi $f \in \mathscr{A}(\boldsymbol{P})$ jest — wobec warunku (1.1) — macierzą trójkątną, tzn. zawierającą same zera poniżej przekątnej głównej. Stąd wniosek, że algebra incydencji n-elementowego zbioru częściowo uporządkowanego jest podalgebrą — właściwą, jeśli $\boldsymbol{P}$ nie jest łańcuchem — algebry macierzy trójkątnych rzeczywistych wymiaru $n \times n$. Warunek $f(x, x) \neq 0$ dla wszystkich $x \in P$, występujący w twierdzeniu 1.2 sprowadza się do żądania, by wyznacznik macierzy $M(f)$, będący oczywiście iloczynem elementów $f(x, x)$, $x \in P$, występujących na przekątnej głównej, był różny od zera.

§ 2. Funkcja Möbiusa i wzór inwersyjny

Obok funkcji δ ważną rolę w algebrze incydencji $\mathscr{A}(P)$ odgrywa funkcja ζ zdefiniowana następująco:

$$\zeta(x, y) = \begin{cases} 1, & \text{jeśli } x \leqslant y, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Innymi słowy, ζ jest funkcją charakterystyczną porządku $\leqslant$. Mamy $\zeta(x, x) \neq 0$ dla dowolnego $x \in P$, a więc w myśl twierdzenia 1.2 element ζ jest odwracalny w $\mathscr{A}(P)$. Odwrotność $\mu = \zeta^{-1}$ nazywamy *funkcją Möbiusa* zbioru częściowo uporządkowanego P. Tak więc

$$\zeta * \mu = \mu * \zeta = \delta,$$

co oznacza, iż

(2.1) $$\mu(x, x) = 1,$$

oraz dla dowolnych $x < y$

(2.2) $$\sum_{z:\, x \leqslant z \leqslant y} \zeta(x, z)\mu(z, y) = \sum_{z:\, x \leqslant z \leqslant y} \mu(z, y) = 0,$$

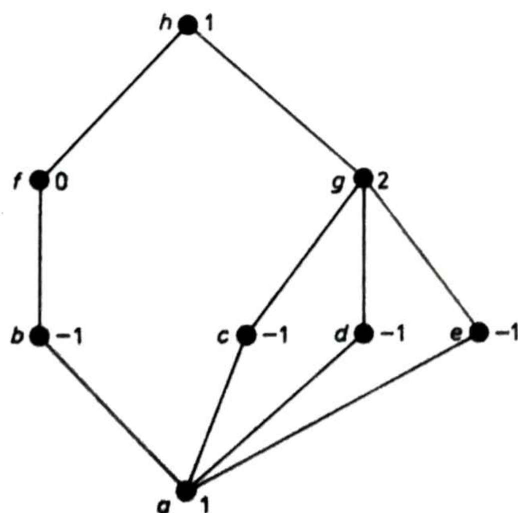
(2.3) $$\sum_{z:\, x \leqslant z \leqslant y} \mu(x, z)\zeta(z, y) = \sum_{z:\, x \leqslant z \leqslant y} \mu(x, z) = 0,$$

czyli

(2.4) $$\mu(x, y) = -\sum_{z:\, x < z \leqslant y} \mu(z, y),$$

(2.5) $$\mu(x, y) = -\sum_{z:\, x \leqslant z < y} \mu(x, z).$$

Każdy z tych dwóch ostatnich wzorów, wraz z (2.1), może służyć do indukcyjnego obliczania funkcji Möbiusa. Zilustrowano to na rysunku 17



$\mu(a, a) = 1$
$\mu(a, b) = (a, c) = (a, d) = (a, e) = -1$
$\mu(a, f) = -(-1+1) = 0$
$\mu(a, g) = -(1-1-1-1) = 2$
$\mu(a, h) = -(1-1-1-1-1+0+2) = 1$

Rys. 17. Wyznaczanie funkcji Möbiusa zbioru częściowo uporządkowanego

(ograniczyliśmy się do obliczenia tylko tych wartości $\mu(x, y)$, dla których $x = a$). Oczywiście funkcja Möbiusa przyjmuje tylko wartości całkowite (ogólniej, dla algebry incydencji złożonej z funkcji o wartościach w dowolnym pierścieniu z jedynką, funkcja Möbiusa przyjmuje wartości z podpierścienia generowanego przez jedynkę; dla pierścienia charakterystyki k podpierścień ten jest oczywiście izomorficzny z pierścieniem $\boldsymbol{Z}_k$ liczb całkowitych modulo k, gdy $k > 0$, lub z pierścieniem $\boldsymbol{Z}$ liczb całkowitych, gdy $k = 0$).

Udowodnimy teraz podstawowy wzór inwersyjny Möbiusa, który będzie stanowił motywację dla badania w następnych paragrafach własności funkcji Möbiusa różnych zbiorów częściowo uporządkowanych. Twierdzenie to zostało w pełnej ogólności podane niezależnie przez Weisnera [1] i P. Halla [2], choć wcześniej znane były jego szczególne przypadki, takie jak klasyczna formuła inwersyjna Möbiusa w teorii liczb, czy też zasada włączania–wyłączania (p. § 1.7). G.-C. Rota w klasycznej pracy [1] na temat algebry incydencji i wzoru inwersyjnego Möbiusa wykazał fundamentalną rolę, jaką pojęcia te odgrywają w kombinatoryce.

Potrzebny nam będzie następujący prosty fakt:

LEMAT 2.1. *Wartość $\mu(x, y)$ zależy jedynie od odcinka $[x, y]$. Co więcej, jeśli odcinek $[x, y]$ jest izomorficzny z odcinkiem $[z, t]$, to $\mu(x, y) = \mu(z, t)$.*

Dowód. Istotnie, ze wzorów (2.1) oraz (2.4) lub (2.5) możemy wyznaczyć $\mu(x, y)$ indukcyjnie, „nie wychodząc" poza odcinek $[x, y]$. Druga część lematu dowodzona jest indukcyjnie ze względu na rangę elementu y w odcinku $[x, y]$, przy wykorzystaniu faktu, iż izomorfizm zachowuje rangę. □

W szczególności, jeśli μ jest funkcją Möbiusa zbioru $\boldsymbol{P} = \langle P, \leqslant \rangle$ oraz $x, y \in P$, to $\mu(x, y) = \mu'(x, y)$, gdzie μ' jest funkcją Möbiusa zbioru $[x, y]$ z porządkiem dziedziczonym z $\boldsymbol{P}$.

Niech $\boldsymbol{P} = \langle P, \leqslant \rangle$ będzie lokalnie skończonym zbiorem częściowo uporządkowanym. Będziemy mówili, że funkcja $F\colon \boldsymbol{P} \to \boldsymbol{R}$ jest *sumowalna* (względem $\leqslant$), jeśli dla każdego $x \in P$ w sumie

$$G(x) = \sum_{y:\, y \leqslant x} F(y) \tag{2.6}$$

występuje tylko skończona liczba składników niezerowych. Zauważmy, że jeśli F jest funkcją sumowalną, to funkcja G określona przez (2.6) jest też sumowalna. Istotnie, jeśli $F(y_1), \ldots, F(y_n)$ są wszystkimi składnikami niezerowymi sumy (2.6), to $G(y) \neq 0$, $y \leqslant x$ może mieć miejsce tylko wtedy, gdy y należy do zbioru $\bigcup_{i=1}^{n} [y_i, x]$, który jest skończony na mocy lokalnej skończoności zbioru $\boldsymbol{P}$. W zastosowaniach mamy często do czynienia z sytuacją, gdy zbiór $\{y \in P\colon y \leqslant x\}$ jest skończony dla każdego $x \in P$; jest tak w szczególności wtedy, gdy nasz zbiór ma element najmniejszy (założenie o lokalnej skończoności pozostaje cały czas w mocy). Wtedy oczywiście każda funkcja $F\colon \boldsymbol{P} \to \boldsymbol{R}$ jest sumowalna.

TWIERDZENIE 2.2 (*wzór inwersyjny Möbiusa*). *Niech* $\boldsymbol{P} = \langle P, \leqslant \rangle$ *będzie lokalnie skończonym zbiorem częściowo uporządkowanym, zaś* $F_=: \boldsymbol{P} \to \boldsymbol{R}$ *funkcją sumowalną względem* $\leqslant$. *Określmy funkcję* $F_\leqslant$ *następująco*:

(2.7) $$F_\leqslant(x) = \sum_{y:y\leqslant x} F_=(y).$$

Wtedy

(2.8) $$F_=(x) = \sum_{y:y\leqslant x} F_\leqslant(y)\mu(y, x),$$

gdzie μ *jest funkcją Möbiusa zbioru* $\boldsymbol{P}$.

Dowód. Utwórzmy zbiór częściowo uporządkowany $\boldsymbol{P}'$ przez dodanie do $\boldsymbol{P}$ nowego elementu m takiego, że

$$m \leqslant x \Leftrightarrow \text{istnieje } y \leqslant x \text{ takie, że } F_=(y) \neq 0.$$

Określmy dodatkowo $F_=(m) = 0$. Łatwo sprawdzić, że $\boldsymbol{P}'$ jest porządkiem lokalnie skończonym. Określmy funkcję $f \in \mathscr{A}(\boldsymbol{P}')$ następująco:

$$f(x, y) = \begin{cases} F_=(y), & \text{jeśli } x = m, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Niech

(2.9) $$g = f * \zeta.$$

Wtedy

$$g(m, y) = \sum_{z:m\leqslant z\leqslant y} f(m, z)\zeta(z, y) = \sum_{z:z\leqslant y} F_=(z) = F_\leqslant(y)$$

(przyjmujemy $F_\leqslant(m) = g(m, m) = 0$). Z równości (2.9) otrzymujemy

$$f = g * \zeta^{-1} = g * \mu,$$

w szczególności

$$F_=(x) = f(m, x) = \sum_{y:m\leqslant y\leqslant x} g(m, y)\mu(y, x) = \sum_{y:m\leqslant y\leqslant x} F_\leqslant(y)\mu(y, x).$$

Równość ta dowodzi twierdzenia, jako że $F_\leqslant(m) = 0$. Użyliśmy tu tego samego symbolu μ do oznaczenia funkcji Möbiusa zbiorów $\boldsymbol{P}$ i $\boldsymbol{P}'$ – mogliśmy tak uczynić wobec lematu 2.1. □

W tym miejscu zauważmy następujący fakt natury algebraicznej. W rodzinie Σ funkcji sumowalnych z P w $\boldsymbol{R}$ wprowadzamy dodawanie „po współrzędnych": $(f+g)(x) = f(x)+g(x)$, oraz mnożenie elementów zbioru Σ przez elementy algebry incydencji $\mathscr{A}(\boldsymbol{P})$ jak następuje: Jeśli $F \in \Sigma$, $f \in \mathscr{A}(\boldsymbol{P})$, to

(2.10) $$(F \odot f)(x) = \sum_{y:y\leqslant x} F(y)f(y, x).$$

Czytelnik zechce sprawdzić następujące fakty:

(a) Działanie $\odot$ jest określone poprawnie, tj. nie wyprowadza ze zbioru Σ.

(b) Σ wraz z działaniami $+$ i $\odot$ jest prawostronnym unitarnym $\mathscr{A}(\boldsymbol{P})$-modułem (por. Białynicki-Birula [1]), w szczególności

$$(F \odot f) \odot g = F \odot (f * g), \tag{2.11}$$

$$F \odot \delta = F. \tag{2.12}$$

Teraz już twierdzenie 2.2 otrzymujemy łatwo w następujący sposób. Jeśli dana jest funkcja sumowania $F_=$, to zdefiniowana wzorem (2.7) funkcja $F_\leqslant$ — to nic innego jak $F_= \odot \zeta$. Mnożąc równość $F_\leqslant = F_= \odot \zeta$ prawostronnie przez funkcję μ i korzystając z (2.11) i (2.12) otrzymujemy

$$F_\leqslant \odot \mu = (F_= \odot \zeta) \odot \mu = F_= \odot (\zeta * \mu) = F_= \odot \delta = F_=.$$

Tak więc $F_= = F_\leqslant \odot \mu$, co jest właśnie algebraicznym równoważnikiem (2.8).

Zauważmy, że z powyższych uwag wynika, iż elementy algebry incydencji działają jako operatory liniowe w przestrzeni funkcji sumowalnych (z działaniami dodawania i mnożenia przez $c \in \boldsymbol{R}$ „po współrzędnych"). Ważną rolę odgrywa w szczególności *operator sumacyjny* S określony przez

$$(SF)(x) = (F \odot \zeta)(x) = \sum_{y:\, y \leqslant x} F(y).$$

Wzór inwersyjny Möbiusa orzeka, iż istnieje operator D odwrotny do S, i wyraża się wzorem

$$(DG)(x) = (G \odot \mu)(x) = \sum_{y:\, y \leqslant x} G(y)\,\mu(y, x).$$

Operator D nazywamy *operatorem różnicowym* w $\boldsymbol{P}$.

Na zakończenie niniejszego paragrafu zauważmy, że wzór inwersyjny Möbiusa jest prawdziwy dla funkcji $F_=$ o wartościach w dowolnej grupie przemiennej G (zapisywanej addytywnie), jeśli iloczyn elementu grupy przez liczbę całkowitą we wzorze (2.8) zdefiniujemy w naturalny sposób:

$$g \cdot 0 = 0, \quad g \cdot (n+1) = g \cdot n + g, \quad g \cdot (-n) = (-g) \cdot n. \tag{2.13}$$

Istotnie, podstawiając (2.7) do (2.8) oraz zmieniając porządek sumowania otrzymujemy

$$\begin{aligned}\sum_{y:\, y \leqslant x} F_\leqslant(y)\,\mu(y, x) &= \sum_{y:\, y \leqslant x} \sum_{z:\, z \leqslant y} F_=(z)\,\mu(y, x) = \\ &= \sum_{z:\, z \leqslant x} \sum_{y:\, z \leqslant y \leqslant x} F_=(z)\,\mu(y, x) = \sum_{z:\, z \leqslant x} F_=(z) \sum_{y:\, z \leqslant y \leqslant x} \mu(y, x) = \\ &= \sum_{z:\, z \leqslant x} F_=(z)\,\delta(z, x) = F_=(x).\end{aligned}$$

Jest to oczywiście również niezależny dowód twierdzenia 2.2. □

Odnotujmy otrzymany wniosek, jako przydatny dla niektórych zastosowań.

TWIERDZENIE 2.3. *Wzór inwersyjny Möbiusa* (2.8) *jest prawdziwy dla funkcji* $F_=$ *o wartościach w dowolnej grupie przemiennej* (*iloczyn elementu grupy przez liczbę całkowitą określamy wzorem* (2.13)).

Zauważmy jeszcze, że jeśli działanie grupowe zapisujemy multyplikatywnie, to twierdzenie 2.3 przyjmuje następującą postać:

Jeśli

(2.14)
$$F_{\leqslant}(x) = \prod_{y:\, y \leqslant x} F_=(y),$$

to

(2.15)
$$F_=(x) = \prod_{y:\, y \leqslant x} F_{\leqslant}(y)\,\mu(y, x)$$

(*o funkcji* $F_=$ *zakładamy, że dla każdego* x *istnieje jedynie skończona liczba elementów* $y \leqslant x$ *takich, że* $F_=(y) \neq 1$).

§ 3. Własności funkcji Möbiusa

W niniejszym paragrafie zajmiemy się podstawowymi własnościami funkcji Möbiusa i korzystając z nich wyznaczymy funkcję Möbiusa dla wielu zbiorów częściowo uporządkowanych. Otrzymamy stąd potem odpowiadające tym zbiorom wersje wzoru inwersyjnego.

O wszystkich rozpatrywanych zbiorach częściowo uporządkowanych zakładamy, że są lokalnie skończone. Funkcję Möbiusa zbioru $\boldsymbol{P}$ będziemy oznaczali niekiedy przez $\mu_{\boldsymbol{P}}$. Przypomnijmy, że porządek dualny do $\boldsymbol{P} = \langle P, \leqslant \rangle$ definiujemy jako $\boldsymbol{P}^* = \langle P, \leqslant^* \rangle$, gdzie $x \leqslant^* y \Leftrightarrow y \leqslant x$.

TWIERDZENIE 3.1. *Jeśli* $\boldsymbol{P}^* = \langle P, \leqslant^* \rangle$ *jest porządkiem dualnym do* $\boldsymbol{P} = \langle P, \leqslant \rangle$, *to*

(3.1)
$$\mu_{\boldsymbol{P}^*}(x, y) = \mu_{\boldsymbol{P}}(y, x).$$

Dowód. Ustalmy element $x \in P$. Wzór (3.1) jest oczywiście prawdziwy dla $y = x$. Niech więc $z > x$, i załóżmy, że jest on prawdziwy dla wszystkich $y < z$. Ze wzorów (2.4), (2.5) otrzymujemy

$$\mu_{\boldsymbol{P}^*}(x, z) = -\sum_{y:\, x \leqslant^* y <^* z} \mu_{\boldsymbol{P}^*}(x, y) = -\sum_{y:\, z < y \leqslant x} \mu_{\boldsymbol{P}}(y, x) = \mu_{\boldsymbol{P}}(z, x).$$

Tak więc twierdzenie wynika z zasady indukcji. □

Inny dowód otrzymujemy bezpośrednio sprawdzając, że funkcja f zdefiniowana przez $f(x, y) = \mu_{\boldsymbol{P}}(y, x)$ jest istotnie odwrotnością funkcji $\zeta_{\boldsymbol{P}^*}$:

$$(\zeta_{\boldsymbol{P}^*} * f)(x, y) = \sum_{z:\, x \leqslant^* z \leqslant^* y} \zeta_{\boldsymbol{P}^*}(x, z) f(z, y) = \sum_{z:\, y \leqslant z \leqslant x} \mu_{\boldsymbol{P}}(y, z) = \delta_{\boldsymbol{P}}(y, x) = \delta_{\boldsymbol{P}^*}(x, y).$$

Odnotujmy jako wniosek z tego twierdzenia wygodną dla zastosowań dualną wersję wzoru inwersyjnego Möbiusa.

TWIERDZENIE 3.2. *Niech* $\boldsymbol{P} = \langle P, \leqslant \rangle$ *będzie lokalnie skończonym zbiorem częściowo uporządkowanym, zaś* $F_{=}\colon P \to \boldsymbol{R}$ *funkcją sumowalną względem* $\geqslant$. *Określmy funkcję* $F_{\geqslant}$ *następująco*:

$$F_{\geqslant}(x) = \sum_{y:\, y \geqslant x} F_{=}(y).$$

Wtedy

$$F_{=}(x) = \sum_{y:\, y \geqslant x} \mu(x, y) F_{\geqslant}(y).$$

Dowód. Jest to bezpośredni wniosek z twierdzenia 2.2 i twierdzenia 3.1. □

Przypomnijmy, że iloczyn kartezjański porządków $\boldsymbol{P}_1 = \langle P_1, \leqslant \rangle$ i $\boldsymbol{P}_2 = \langle P_2, \leqslant \rangle$ definiujemy następująco:

$$\boldsymbol{P}_1 \times \boldsymbol{P}_2 = \langle P_1 \times P_2, \leqslant \rangle,$$

przy czym

$$\langle x, y \rangle \leqslant \langle z, t \rangle \Leftrightarrow x \leqslant z \wedge y \leqslant t.$$

Okazuje się, że funkcję Möbiusa iloczynu kartezjańskiego można wyznaczyć w bardzo prosty sposób znając funkcje Möbiusa czynników.

TWIERDZENIE 3.3. *Jeśli* $\boldsymbol{P}_1$, $\boldsymbol{P}_2$ *są porządkami lokalnie skończonymi, to*

$$\mu_{\boldsymbol{P}_1 \times \boldsymbol{P}_2}(\langle x, y \rangle, \langle z, t \rangle) = \mu_{\boldsymbol{P}_1}(x, z)\, \mu_{\boldsymbol{P}_2}(y, t). \tag{3.2}$$

Dowód. Oczywiście

$$\mu_{\boldsymbol{P}_1 \times \boldsymbol{P}_2}(\langle x, y \rangle, \langle x, y \rangle) = 1 = \mu_{\boldsymbol{P}_1}(x, x)\, \mu_{\boldsymbol{P}_2}(y, y).$$

Niech $\langle u, v \rangle > \langle x, y \rangle$. Przyjmując jako założenie indukcyjne prawdziwość wzoru (3.2) dla wszystkich $\langle z, t \rangle < \langle u, v \rangle$ i korzystając ze wzoru (2.5) otrzymujemy

$$\begin{aligned}
\mu_{\boldsymbol{P}_1 \times \boldsymbol{P}_2}(\langle x, y \rangle, \langle u, v \rangle) &= - \sum_{\langle z,t \rangle:\, \langle x,y \rangle \leqslant \langle z,t \rangle < \langle u,v \rangle} \mu_{\boldsymbol{P}_1 \times \boldsymbol{P}_2}(\langle x, y \rangle, \langle z, t \rangle) = \\
&= - \sum_{\langle z,t \rangle:\, \langle x,y \rangle \leqslant \langle z,t \rangle < \langle u,v \rangle} \mu_{\boldsymbol{P}_1}(x, z)\, \mu_{\boldsymbol{P}_2}(y, t) = \\
&= \Big(- \sum_{\langle z,t \rangle:\, \langle x,y \rangle \leqslant \langle z,t \rangle \leqslant \langle u,v \rangle} \mu_{\boldsymbol{P}_1}(x, z)\, \mu_{\boldsymbol{P}_2}(y, t)\Big) + \mu_{\boldsymbol{P}_1}(x, u)\, \mu_{\boldsymbol{P}_2}(y, v) = \\
&= \Big(- \sum_{z:\, x \leqslant z \leqslant u} \mu_{\boldsymbol{P}_1}(x, z) \sum_{t:\, y \leqslant t \leqslant v} \mu_{\boldsymbol{P}_2}(y, t) + \mu_{\boldsymbol{P}_1}(x, u)\, \mu_{\boldsymbol{P}_2}(y, v) = \\
&= -\delta_{\boldsymbol{P}_1}(x, u)\, \delta_{\boldsymbol{P}_2}(y, v) + \mu_{\boldsymbol{P}_1}(x, u)\, \mu_{\boldsymbol{P}_2}(y, v) = \mu_{\boldsymbol{P}_1}(x, u)\, \mu_{\boldsymbol{P}_2}(y, v),
\end{aligned}$$

gdyż założyliśmy $\langle x, y \rangle < \langle u, v \rangle$. □

Nieco prostszy dowód otrzymujemy bezpośrednio sprawdzając, że funkcja $f \in \mathscr{A}(\boldsymbol{P}_1 \times \boldsymbol{P}_2)$ zdefiniowana przez

$$f(\langle x, y\rangle, \langle z, t\rangle) = \mu_{\boldsymbol{P}_1}(x, z)\mu_{\boldsymbol{P}_2}(y, t)$$

jest istotnie odwrotnością elementu $\zeta_{\boldsymbol{P}_1 \times \boldsymbol{P}_2}$ w algebrze $\mathscr{A}(\boldsymbol{P}_1 \times \boldsymbol{P}_2)$:

$$\begin{aligned}(\zeta_{\boldsymbol{P}_1\times\boldsymbol{P}_2} * f)(\langle x, y\rangle, \langle u, v\rangle) &= \\ &= \sum_{\langle z,t\rangle:\ \langle x,y\rangle \leqslant \langle z,t\rangle \leqslant \langle u,v\rangle} \zeta_{\boldsymbol{P}_1\times\boldsymbol{P}_2}(\langle x, y\rangle, \langle z, t\rangle)\mu_{\boldsymbol{P}_1}(z, u)\mu_{\boldsymbol{P}_2}(t, v) = \\ &= \sum_{z:\ x\leqslant z\leqslant u} \mu_{\boldsymbol{P}_1}(z, u) \sum_{t:\ y\leqslant t\leqslant v} \mu_{\boldsymbol{P}_2}(t, v) = \\ &= \delta_{\boldsymbol{P}_1}(x, u)\delta_{\boldsymbol{P}_2}(y, v) = \delta_{\boldsymbol{P}_1\times\boldsymbol{P}_2}(\langle x, y\rangle, \langle u, v\rangle).\end{aligned}$$

Twierdzenie to przenosi się w oczywisty sposób na iloczyn dowolnej skończonej liczby porządków. Korzystamy tu milcząco z faktu, iż iloczyn kartezjański skończonej liczby porządków lokalnie skończonych jest lokalnie skończony. Własność ta na ogół nie przenosi się na iloczyn nieskończonej liczby czynników (p. zad. 8). Załóżmy teraz, że porządki $\boldsymbol{P}_i$, $i \in I$, są lokalnie skończone oraz każdy z nich ma zero (element najmniejszy), które oznaczamy przez 0 (użycie tego samego symbolu dla oznaczenia zera w każdym ze zbiorów $\boldsymbol{P}_i$ nie prowadzi do nieporozumień). Wtedy lokalnie skończona jest również suma prosta $\bigoplus_{i\in I} \boldsymbol{P}_i$ (p. tw. 1.2.2). Przypomnijmy, że tę sumę prostą określamy jako zbiór tych elementów $x \in \bigtimes_{i\in I} \boldsymbol{P}_i$, dla których zbiór $I_x = \{i \in I:\ x_i \neq 0\}$ jest skończony. Łatwo zauważyć, że jeśli $x \leqslant y$, $y \neq 0$, to odcinek $[x, y]$ zbioru $\bigoplus_{i\in I} \boldsymbol{P}_i$ jest izomorficzny z odcinkiem $[\bar{x}, \bar{y}]$ zbioru $\bigtimes_{i\in I_y} \boldsymbol{O}_i$, gdzie $\bar{x}_i = x_i$, $\bar{y}_i = y_i$ dla $i \in I_y$.

Korzystając z poprzedniego twierdzenia możemy więc obliczyć funkcję Möbiusa w sumie prostej:

TWIERDZENIE 3.4. *Jeśli $\boldsymbol{P} = \bigoplus_{i\in I} \boldsymbol{P}_i$, gdzie porządki $\boldsymbol{P}_i$ są lokalnie skończone, to dla dowolnych elementów x, y tej sumy takich, że $x \leqslant y$ mamy*

$$\mu_{\boldsymbol{P}}(x, y) = \prod_{i\in I_y} \mu_{\boldsymbol{P}_i}(x_i, y_i). \ \square$$

Twierdzenia 3.3 i 3.4 umożliwiają wyznaczanie funkcji Möbiusa skomplikowanego zbioru częściowo uporządkowanego przez jego rozkład na iloczyn lub sumę prostą zbiorów o prostej strukturze. Podamy teraz jeszcze jeden fakt, który jest pomocny przy obliczaniu funkcji Möbiusa w przypadku, gdy nasz zbiór częściowo uporządkowany jest kratą.

TWIERDZENIE 3.5 (Weisner [1]). *Niech μ będzie funkcją Möbiusa kraty skończonej L, oraz niech $a, b \in L$.*

(a) *Jeśli* $a > 0$, *to*

$$\sum_{x:\, x \vee a = b} \mu(0, x) = 0. \tag{3.3}$$

(b) *Jeśli* $a < 1$, *to*

$$\sum_{x:\, x \wedge a = b} \mu(x, 1) = 0. \tag{3.4}$$

Dowód. (a) Jeśli $a \nleqslant b$, to $\{x\colon x \vee a = b\} = \emptyset$ i oczywiście twierdzenie nasze jest prawdziwe. Załóżmy więc, że $a \leqslant b$. Jeśli twierdzenie jest fałszywe, to możemy wybrać takie minimalne b, że suma po prawej stronie (3.3) jest niezerowa. Mamy wtedy

$$\sum_{x:\, x \vee a \leqslant b} \mu(0, x) = \sum_{x:\, x \vee a = b} \mu(0, x) + \sum_{c:\, c < b} \sum_{x:\, x \vee a = c} \mu(0, x). \tag{3.5}$$

Lecz $x \vee a \leqslant b$ oznacza dokładnie tyle, co $0 \leqslant x \leqslant b$, a więc zgodnie z (2.3) lewa strona jest równa zeru. Druga część prawej strony jest również równa zeru, na mocy wyboru elementu b. Tak więc (3.5) redukuje się do

$$0 = \sum_{x:\, x \vee a = b} \mu(0, x),$$

wbrew naszemu założeniu.

Część (b) otrzymujemy rozważając porządek dualny do $\leqslant$ i korzystając z twierdzenia 3.1. □

Przystępujemy teraz do wyznaczania funkcji Möbiusa dla konkretnych zbiorów częściowo uporządkowanych.

A. *Zbiory liniowo uporządkowane*. Niech $\boldsymbol{P} = \langle P, \leqslant \rangle$ będzie (lokalnie skończonym) zbiorem liniowo uporządkowanym. Rozważmy jego dowolny odcinek $\{x_1, \ldots, x_n\}$, gdzie $x_1 < \ldots < x_n$. Zgodnie z wzorami (2.1) i (2.5) mamy

$$\mu(x_1, x_1) = 1,$$
$$\mu(x_1, x_2) = -\mu(x_1, x_1) = -1,$$
$$\mu(x_1, x_3) = -(\mu(x_1, x_1) + \mu(x_1, x_2)) = -(1-1) = 0$$

i ogólnie

$$\mu(x_1, x_k) = 0 \quad \text{dla } k \geqslant 3.$$

Mamy stąd następujące twierdzenie:

TWIERDZENIE 3.6. *Funkcja Möbiusa zbioru liniowo uporządkowanego jest równa*

$$\mu(x, y) = \begin{cases} 1, & \textit{jeśli } x = y, \\ -1, & \textit{jeśli } y \textit{ jest bezpośrednim następnikiem elementu } x, \\ 0, & \textit{w pozostałych przypadkach.} \end{cases}$$ □

Warto zauważyć, że zgodnie z tym twierdzeniem zastosowanie wzoru inwersyjnego (2.8) do zbioru liczb naturalnych z porządkiem naturalnym daje po prostu

$$F_{\leqslant}(n) = \sum_{i=1}^{n} F_{=}(i) \Rightarrow F_{=}(n) = F_{\leqslant}(n) - F_{\leqslant}(n-1).$$

Przy dowodzeniu twierdzenia 3.6 korzystaliśmy jedynie z faktu, że każdy odcinek jest łańcuchem. Zatem twierdzenie to pozostaje w mocy dla znacznie szerszej klasy porządków częściowych niż porządki liniowe, np. dla porządków o strukturze drzewa.

B. *Podzbiory skończone ustalonego zbioru.* Dla dowolnego zbioru X zbiór częściowo uporządkowany $\langle \mathscr{P}_{\text{fin}}(X), \subseteq \rangle$ jest lokalnie skończony. Jest on izomorficzny z sumą prostą $|X|$ kopii zbioru $\langle \{0, 1\}, \leqslant \rangle$, gdyż dowolny podzbiór $A \subseteq_{\text{fin}} X$ możemy identyfikować z funkcją $\chi_A \colon X \to \{0, 1\}$ taką, że

$$\chi_A(x) = \begin{cases} 1, & \text{jeśli } x \in A, \\ 0, & \text{jeśli } x \notin A. \end{cases}$$

Wobec twierdzenia 3.6 postać funkcji Möbiusa dla zbioru $\langle \{0, 1\}, \leqslant \rangle$ jest następująca

$$\mu(0, 0) = \mu(1, 1) = 1, \qquad \mu(0, 1) = -1.$$

Korzystając z twierdzenia 3.4 łatwo już otrzymujemy wzór na funkcję Möbiusa zbioru $\langle \mathscr{P}_{\text{fin}}(X), \subseteq \rangle$.

TWIERDZENIE 3.7. *Funkcja Möbiusa zbioru $\langle \mathscr{P}_{\text{fin}}(X), \subseteq \rangle$ wyraża się wzorem*

$$\mu(A, B) = \begin{cases} (-1)^{|B|-|A|}, & \textit{jeśli } A \subseteq B, \\ 0, & \textit{w przeciwnym przypadku}. \end{cases} \quad \square$$

C. *Liczby naturalne z relacją podzielności.* Niech $p_1, p_2, \ldots$ będzie ciągiem kolejnych liczb pierwszych. Na mocy twierdzenia o jednoznacznym rozkładzie dowolnej liczby naturalnej na czynniki pierwsze, zbiór $\langle \boldsymbol{N}, | \rangle$ jest izomorficzny z sumą prostą $\bigoplus_{i=1}^{\infty} \boldsymbol{P}_i$, gdzie każde $\boldsymbol{P}_i$ jest nieskończonym łańcuchem $0 < 1 < 2 < \ldots$ Istotnie, każdej liczbie n możemy jednoznacznie przyporządkować element α naszej sumy prostej taki, że $\prod_{i \in I_\alpha} p_i^{\alpha_i}$ jest rozkładem kanonicznym liczby n. Łatwo zauważyć, że jeśli przy tym przyporządkowaniu α odpowiada liczbie n, β zaś liczbie m, to

$$n|m \Leftrightarrow \alpha \leqslant \beta \qquad (\text{tzn. } \alpha_i \leqslant \beta_i \text{ dla każdego } i).$$

Wobec twierdzenia 3.6 wiemy, jaka jest postać funkcji Möbiusa dla łańcuchów $\boldsymbol{P}_i$.

Wystarczy teraz skorzystać z twierdzenia 3.4, aby otrzymać wzór na funkcję Möbiusa zbioru $\langle N, |\rangle$:

$$\mu(n, m) = \prod_{i \in I_\beta} \mu_{p_i}(\alpha_i, \beta_i) =$$

$$= \begin{cases} (-1)^{\sum_{i \in I_\beta}(\beta_i - \alpha_i)}, & \text{jeśli } \beta_i - \alpha_i \leqslant 1 \text{ dla każdego } i \in I_\beta, \\ 0, & \text{w przeciwnym przypadku,} \end{cases}$$

gdzie $n|m$, $n = \prod_{i \in I_\alpha} p_i^{\alpha_i}$, $m = \prod_{i \in I_\beta} p_i^{\beta_i}$. Mamy stąd

TWIERDZENIE 3.8. *Funkcja Möbiusa zbioru* $\langle N, |\rangle$ *jest równa*

$$\mu(n, m) = \begin{cases} (-1)^k, & \text{jeśli } n|m \text{ i } m/n \text{ jest iloczynem } k \text{ różnych liczb pierwszych,} \\ 0, & \text{w przeciwnym przypadku.} \end{cases} \square$$

D. *Podziały zbioru.* Obliczymy teraz funkcję Möbiusa dla zbioru $\langle \Pi(X), \leqslant\rangle$. Przypomnijmy, że $\Pi(X)$ oznacza zbiór wszystkich podziałów zbioru X, oraz że $\pi \leqslant \sigma$ oznacza, iż podział π jest drobniejszy niż σ, tzn. każdy blok podziału σ jest sumą pewnej liczby bloków podziału π. Bez zmniejszenia ogólności możemy zakładać w naszych rozważaniach, że $X = \{1, \ldots, n\}$. Będziemy w takim przypadku używali oznaczenia $\Pi(X) = \Pi_n$. Udowodnimy najpierw następujący prosty lemat.

LEMAT 3.9. *Niech* $\pi, \sigma \in \Pi_n$, $\pi \leqslant \sigma$. *Załóżmy, że* $|\sigma| = k$ *oraz* j*-ty blok podziału* σ *jest sumą* n_j *bloków podziału* π, $1 \leqslant j \leqslant k$. *Wtedy*

$$[\pi, \sigma] \simeq \Pi_{n_1} \times \ldots \times \Pi_{n_k}.$$

Dowód. Niech $\sigma = \{B_1, \ldots, B_k\}$. Każdy blok B_j jest sumą n_j bloków podziału π:

$$B_j = A_{j1} \dot{\cup} \ldots \dot{\cup} A_{jn_j}, \qquad \text{gdzie } A_{jl} \in \pi \text{ dla } 1 \leqslant l \leqslant n_j.$$

Dowolny podział τ taki, że $\pi \leqslant \tau \leqslant \sigma$ jest jednoznacznie wyznaczony przez podziały

$$\tau_j = \{B_j\colon C \in \tau \wedge C \subseteq B_j\}, \qquad 1 \leqslant j \leqslant k,$$

które indukuje on na blokach podziału σ. Skoro rozważamy tylko podziały $\tau \geqslant \pi$, to możemy z kolei każdemu podziałowi τ_j jednoznacznie przyporządkować podział $\bar{\tau}_j \in \Pi_{n_j}$ powstały z τ_j przez zastąpienie każdego bloku $C \in \tau_j$ przez

$$\bar{C} = \{l\colon A_{jl} \subseteq C\}.$$

Łatwo sprawdzić, że opisane przez nas odwzorowanie $\tau \mapsto \langle \bar{\tau}_1, \ldots, \bar{\tau}_k \rangle$ określa izomorfizm przedziału $[\pi, \sigma]$ z iloczynem $\Pi_{n_1} \times \ldots \times \Pi_{n_k}$. $\square$

Wobec lematu 3.9 i twierdzenia 3.2

(3.6) $$\mu_{\Pi_n}(\pi, \sigma) = \prod_{j=1}^{k} \mu_{\Pi_{n_j}}(0, 1),$$

gdzie przez 0 i 1 oznaczamy odpowiednio podział „najdrobniejszy" na bloki jednoelementowe oraz podział „najgrubszy" składający się z jednego bloku. Zauważmy, że zarówno 0 jak i 1 może oznaczać różne podziały w różnych czynnikach iloczynu (3.6).

Wystarczy teraz obliczyć $\mu_{\Pi_n}(0, 1)$ dla dowolnego n. Jak wiemy, podziały zbioru tworzą kratę, przy czym

$$\pi \wedge \sigma = \{A \cap B \colon A \in \pi \wedge B \in \sigma \wedge A \cap B \neq \emptyset\}$$

(p. tw. 1.8.1). Możemy więc skorzystać z twierdzenia Weisnera (twierdzenie 3.4). Niech π będzie następującym elementem kraty Π_n, $n > 1$:

$$\pi = \{\{1, \ldots, n-1\}, \{n\}\}.$$

Przyjmijmy w twierdzeniu Weisnera (część (b)) $a = \pi$, $b = 0$ (tzn. $b = \{\{1\}, \ldots, \{n\}\}$), i zobaczmy co oznacza równość $x \wedge a = b$, tzn. $x \wedge \pi = 0$. Skoro bloki podziału $x \wedge \pi$ są przecięciami bloków podziału x z blokami podziału π, to oznacza ona dokładnie tyle, że $x = 0$ lub x jest podziałem na $n-1$ bloków postaci

$$\sigma_j = \{\{1\}, \{2\}, \ldots, \{j-1\}, \{j+1\}, \ldots, \{n-1\}, \{j, n\}\}, \qquad 1 \leqslant j \leqslant n-1.$$

Z twierdzenia Weisnera dostajemy więc

(3.7) $$\mu_{\Pi_n}(0, 1) + \sum_{j=1}^{n-1} \mu_{\Pi_n}(\sigma_j, 1) = 0.$$

Lecz z lematu 3.9 wynika, że każdy z odcinków $[\sigma_j, 1]$ w Π_n jest izomorficzny z Π_{n-1}. Zatem z (3.7) otrzymujemy wzór rekurencyjny

$$\mu_{\Pi_n}(0, 1) = -(n-1)\,\mu_{\Pi_{n-1}}(0, 1),$$

który po uwzględnieniu równości $\mu_{\Pi_1}(0, 1) = 1$ daje

(3.8) $$\mu_{\Pi_n}(0, 1) = (-1)^{n-1}(n-1)!.$$

Podstawiając tę równość do (3.6) otrzymujemy ostatecznie

TWIERDZENIE 3.10 (Schützenberger [1], Rota [2]). *Funkcja Möbiusa kraty Π_n wyraża się wzorem*

$$\mu(\pi, \sigma) = (-1)^{|\pi| - |\sigma|} \prod_{j=1}^{|\sigma|} (n_j - 1)!$$

dla dowolnych $\pi \leqslant \sigma$, przy czym n_j oznacza liczbę bloków podziału π zawartych w j-tym bloku podziału σ. □

Pokażemy jeszcze inny sposób wyznaczania funkcji Möbiusa dla kraty podziałów. Polega on na zastosowaniu metody współczynników nieoznaczonych do wzoru inwersyjnego. Niech $X = \{1, \ldots, n\}$ i niech Y będzie dowolnym zbiorem. Przypomnijmy, że każdej funkcji $f\colon X \to Y$ odpowiada podział $N(f) \in \Pi(X)$, zwany jej jądrem:

$$N(f) = \{f^{-1}(y)\colon\ y \in Y \wedge f^{-1}(y) \neq \emptyset\}.$$

Oznaczmy przez $F_{=}(\pi)$ liczbę funkcji $f\colon X \to Y$ takich, że $N(f) = \pi$, a przez $F_{\geqslant}(\pi)$ takich, że $N(f) \geqslant \pi$. Oczywiście

$$F_{\geqslant}(\pi) = \sum_{\sigma:\,\sigma \geqslant \pi} F_{=}(\sigma),$$

a więc zgodnie z twierdzeniem 3.2

$$F_{=}(\pi) = \sum_{\sigma:\,\sigma \geqslant \pi} \mu(\pi, \sigma) F_{\geqslant}(\sigma).$$

W szczególności

(3.9) $$F_{=}(0) = \sum_{\sigma \in \Pi_n} \mu(0, \sigma) F_{\geqslant}(\sigma).$$

Lecz $F_{=}(0)$ to nic innego jak liczba funkcji różnowartościowych $f\colon X \to Y$, a więc $F_{=}(0) = [x]_n$, gdzie $x = |Y|$. Z kolei każda funkcja f taka, że $N(f) \geqslant \sigma$ wyznaczona jest jednoznacznie przez podanie elementów zbioru Y, na które przechodzą elementy każdego z bloków $B \in \sigma$ (różne bloki mogą przechodzić na ten sam element). Takich funkcji jest więc $x^{|\sigma|}$. Równość (3.9) możemy więc przepisać jako

(3.10) $$x(x-1)\ldots(x-n+1) = \sum_{\sigma \in \Pi_n} \mu(0, \sigma) x^{|\sigma|}.$$

Równość ta zachodzi dla każdego $x > 0$ całkowitego, gdyż zbiór Y może być dowolny. A więc wielomiany zmiennej x po obu stronach (3.10) są równe. Porównując współczynniki przy x otrzymujemy (3.8). Zauważmy przy okazji, że współczynnik przy x^k w (3.10) jest równy $\sum_{\sigma:\,|\sigma| = k} \mu(0, \sigma)$. Z drugiej strony wiemy, że $[x]_n = \sum_{k-1}^{n} s(n, k) x^k$, gdzie $s(n, k)$ są liczbami Stirlinga pierwszego rodzaju (p. (1.4.11)). Otrzymujemy stąd następującą równość (pochodzącą od Roty [1]):

(3.11) $$s(n, k) = \sum_{\sigma:\,|\sigma| = k} \mu(0, \sigma).$$

Do zależności tej powrócimy jeszcze w następnym paragrafie.

E. *Podprzestrzenie przestrzeni liniowej.* Wyznaczymy teraz funkcję Möbiusa dla $\mathscr{L}(n, q)$. Przypomnijmy, że przez $\mathscr{L}(n, q)$ oznaczamy kratę wszystkich podprzestrzeni n-wymiarowej przestrzeni liniowej $V(n, q)$. Można tu skorzystać z

twierdzenia Weisnera, w podobny sposób jak w przypadku kraty podziałów, można również zastosować do wzoru inwersyjnego metodę współczynników nieoznaczonych. Pokażemy ten drugi sposób, gdyż dostarcza on pewnych dodatkowych informacji.

Niech Y będzie dowolną przestrzenią liniową nad ciałem $GF(q)$. Dla dowolnej podprzestrzeni $Z \subseteq V(n, q)$ oznaczmy przez $F_=(Z)$ liczbę odwzorowań liniowych $f\colon V(n, q) \to Y$, których jądrem jest Z (tzn. $f^{-1}(0) = Z$). Podobnie, niech $F_\geqslant(Z)$ oznacza liczbę odwzorowań liniowych $f\colon V(n, q) \to Y$, dla których $Z \subseteq f^{-1}(0)$. Mamy

$$F_\geqslant(Z) = \sum_{T\colon T \supseteq Z} F_=(T),$$

a więc zgodnie ze wzorem inwersyjnym

$$F_=(Z) = \sum_{T\colon T \supseteq Z} \mu(Z, T) F_\geqslant(T),$$

co dla $Z = 0$ daje

(3.12) $$F_=(0) = \sum_{T \in \mathscr{L}(n,q)} \mu(0, T) F_\geqslant(T).$$

Zauważmy, że $F_=(0)$ jest liczbą różnowartościowych odwzorowań liniowych $f\colon V(n, q) \to Y$. Każde takie odwzorowanie określone jest jednoznacznie przez ciąg n liniowo niezależnych wektorów przestrzeni Y, jeśli ciąg taki traktować jako obraz ustalonej bazy $e_1, \ldots, e_n$ przestrzeni $V(n, q)$. Oznaczmy $|Y| = x$. Wektor $f(e_1)$ możemy wybrać na $x-1$ sposobów. Rozpina on jednowymiarową podprzestrzeń złożoną z q wektorów, $f(e_2)$ możemy zatem wybrać na $x-q$ sposobów, podobnie $f(e_3)$ na $x-q^2$ sposobów itd. Stąd $F_=(0) = (x-1)(x-q)(x-q^2)\ldots(x-q^{n-1})$. Aby obliczyć $F_\geqslant(T)$, załóżmy, że $e_1, \ldots, e_n$ jest bazą przestrzeni $V(n, q)$ taką, że $e_1, \ldots, e_{\dim T}$ jest bazą przestrzeni T. Warunek $T \subseteq f^{-1}(0)$ oznacza, że $f(e_1) = \ldots = f(e_{\dim T}) = 0$, natomiast $f(e_i)$, $\dim T \leqslant i \leqslant n$, są dowolnymi elementami przestrzeni Y. Stąd $F_\geqslant(T) = x^{n-\dim T}$. Jeśli teraz uwzględnimy fakt, że odcinki $[0, T]$, $[0, T']$ kraty $\mathscr{L}(n, q)$ są izomorficzne, ilekroć $\dim T = \dim T'$, to wzór (3.12) możemy przepisać jako

(3.13) $$(x-1)(x-q)(x-q^2)\ldots(x-q^{n-1}) = \sum_{T \in \mathscr{L}(n,q)} \mu(0, T) x^{n-\dim T} = \sum_{k=0}^{n} \binom{n}{k}_q \mu_{\mathscr{L}(k,q)}(0, 1) x^{n-k}.$$

Równość ta jest spełniona dla nieskończenie wielu wartości x, bowiem $x = |Y|$, Y zaś jest przestrzenią dowolnego wymiaru nad $GF(q)$. Mamy więc do czynienia z równością dwóch wielomianów zmiennej x. Porównując współczynniki przy wyrazie wolnym po obu stronach otrzymujemy

(3.14) $$\mu_{\mathscr{L}(n,q)}(0, 1) = (-1)(-q)(-q^2)\ldots(-q^{n-1}) = (-1)^n q^{n(n-1)/2} = (-1)^n q^{\binom{n}{2}}.$$

Zauważmy, że jeśli Z jest podprzestrzenią przestrzeni T, to odcinek $[Z, T]$ jest izomorficzny z kratą $\mathscr{L}(k, q)$, gdzie $k = \dim T - \dim Z$. Aby się o tym przekonać, rozważmy zbiór T/Z wszystkich warstw przestrzeni T względem podprzestrzeni Z. Na zbiorze tym możemy, jak łatwo sprawdzić, wprowadzić strukturę przestrzeni liniowej wymiaru k definiując $A+B = \{a+b\colon a\in A \wedge b\in B\}$, $\lambda A = \{\lambda a\colon a\in A\}$ dla dowolnych $A, B\in T/Z$, $\lambda\in GF(q)$. Żądany izomorfizm między odcinkiem $[Z, T]$ a kratą podprzestrzeni przestrzeni T/Z otrzymujemy przyporządkowując podprzestrzeni $U\in[Z, T]$ zbiór $\{A\in T/Z\colon A\subseteq U\}$, który oczywiście jest podprzestrzenią przestrzeni T/Z. Zatem $\mu(Z, T) = \mu_{\mathscr{L}(k,q)}(0, 1)$ i ostatecznie otrzymujemy

TWIERDZENIE 3.11. *Funkcja Möbiusa kraty $\mathscr{L}(n, q)$ wyraża się wzorem*

$$\mu(Z, T) = (-1)^k q^{\binom{k}{2}}, \qquad k = \dim T - \dim Z$$

dla dowolnych Z, $T\in\mathscr{L}(n, q)$ takich, że $Z\subseteq T$. □

Podstawiając tę wartość funkcji Möbiusa do (3.13) otrzymujemy tożsamość

(3.14) $$\prod_{k=0}^{n-1}(x-q^k) = \sum_{k=0}^{n}\binom{n}{k}_q(-1)^k q^{\binom{k}{2}} x^{n-k}.$$

§ 4. Wielomian charakterystyczny zbioru częściowo uporządkowanego

Niech $\boldsymbol{P} = \langle P, \leqslant\rangle$ będzie dowolnym skończonym zbiorem częściowo uporządkowanym z zerem 0 i jedynką 1. Przez $r(a)$ będziemy oznaczali, jak zwykle, rangę elementu a, tzn. maksymalną liczność łańcucha w $[0, a]$ zmniejszoną o jeden. Niech $r(1) = n$. *Wielomian charakterystyczny* zbioru $\boldsymbol{P}$ definiujemy następująco:

(4.1) $$\chi_{\boldsymbol{P}}(x) = \sum_{a\in P}\mu(0, a)\,x^{n-r(a)}.$$

Współczynnik przy x^{n-k}, tzn.

(4.2) $$w_{\boldsymbol{P}}(k) = \sum_{a\colon r(a)=k}\mu(0, a),$$

nazywamy *k-tym współczynnikiem pierwszego rodzaju* (dla zbioru $\boldsymbol{P}$). Definiujemy również *k-ty współczynnik drugiego rodzaju*:

(4.3) $$W_p(k) = |\{a\in P\colon r(a) = k\}|.$$

Widać tu pewną analogię do liczb Stirlinga pierwszego i drugiego rodzaju, gdyż jeśli $\boldsymbol{P} = \Pi_n$, to $w_{\boldsymbol{P}}(k) = s(n, n-k)$, $W_{\boldsymbol{P}}(k) = S(n, n-k)$. Wynika to z faktu, iż $r(\sigma) = n-|\sigma|$, oraz ze wzoru (3.11). Okazuje się, że analogia ta sięga znacznie dalej. Aby ją wyjaśnić, załóżmy, że $\boldsymbol{P}_0, \boldsymbol{P}_1, \boldsymbol{P}_2, \ldots$ jest ciągiem skończonym zbiorów częściowo uporządkowanych z zerem i jedynką takich, że dla każdego n

(α) $r(\boldsymbol{P}_n) = n$ ($r(\boldsymbol{P}_n)$ oznacza rangę jedynki w $\boldsymbol{P}_n$),

(β) dla dowolnego $k \leqslant n$ oraz dla dowolnego elementu $a \in P_n$ rangi $n-k$ odcinek $[a, 1]$ zbioru P_n jest izomorficzny z P_k.

Przyjmijmy teraz

$$w(n, k) = \begin{cases} w_{P_n}(k), & \text{jeśli } 0 \leqslant k \leqslant n, \\ 0, & \text{w przeciwnym przypadku,} \end{cases}$$

$$W(n, k) = \begin{cases} W_{P_n}(k), & \text{jeśli } 0 \leqslant k \leqslant n, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

TWIERDZENIE 4.1. *Dla dowolnych ciągów* $a_0, a_1, a_2, \ldots$ *oraz* $b_0, b_1, b_2, \ldots$

$$b_n = \sum_{k=0}^{n} W(n, n-k)\, a_k, \qquad n = 1, 2, \ldots \Leftrightarrow$$

$$\Leftrightarrow a_n = \sum_{k=0}^{n} w(n, n-k)\, b_k, \qquad n = 1, 2, \ldots$$

Wyrazy a_i, b_i *mogą być elementami dowolnego pierścienia charakterystyki zero (a nawet dowolnej grupy przemiennej* — por. (2.13)).

Dowód. Twierdzenie mówi dokładnie tyle, że dla dowolnego n macierz $[w_{ij}]$, $0 \leqslant i, j \leqslant n$, $w_{ij} = w(i, i-j)$, jest odwrotnością macierzy $[W_{ij}]$, $0 \leqslant i, j \leqslant n$, $W_{ij} = W(i, i-j)$. Tak jest w istocie, gdyż

$$\sum_{k=0}^{n} W_{ik} w_{kj} = \sum_{k=0}^{n} W(i, i-k)\, w(k, k-j) = \sum_{k=0}^{n} W(i, i-k) \sum_{\substack{b \in P_k \\ r(b) = k-j}} \mu(0, b) =$$

$$= \sum_{k=0}^{i} \sum_{\substack{a \in P_i \\ r(a) = i-k}} \sum_{\substack{b \in [a, 1] \\ r(b) = (i-k)+(k-j)}} \mu(a, b) =$$

$$= \sum_{a \in P_i} \sum_{\substack{b \in [a, 1] \\ r(b) = i-j}} \mu(a, b) = \sum_{b:\, r(b) = i-j} \sum_{a:\, 0 \leqslant a \leqslant b} \mu(a, b) = \delta_{ij}. \ \square$$

Zauważmy, że używaliśmy tu tego samego symbolu μ dla oznaczenia funkcji Möbiusa różnych zbiorów częściowo uporządkowanych. Mogliśmy tak uczynić wobec warunku (β) i lematu 2.1.

Wyrazy a_i, b_i mogą być dowolnymi wielomianami o współczynnikach rzeczywistych, i wobec

(4.4) $$\chi_{P_n}(x) = \sum_{k=0}^{n} w(n, n-k)\, x^k$$

otrzymujemy

(4.5) $$x^n = \sum_{k=0}^{n} W(n, n-k)\, \chi_{P_k}(x).$$

W przypadku $\boldsymbol{P}_n = \Pi_n$ zależności te wraz z równościami $w(n, n-k) = s(n, k)$, $W(n, n-k) = S(n, k)$ dają znane wzory

$$[x]_n = \sum_{k=0}^{n} s(n, k)x^k, \qquad x^n = \sum_{k=0}^{n} S(n, k)[x]_k.$$

Oczywiście korzystamy tu z faktu, że warunki (α), (β) dotyczące ciągu $\boldsymbol{P}_0, \boldsymbol{P}_1, \ldots$ są spełnione, gdy $\boldsymbol{P}_n = \Pi_n$. Łatwo zauważyć, że są one również spełnione, gdy $\boldsymbol{P}_n = \mathscr{P}_n$ oraz gdy $\boldsymbol{P}_n = \mathscr{L}(n, q)$. Obliczymy teraz współczynniki pierwszego i drugiego rodzaju dla $\mathscr{P}_n$ oraz $\mathscr{L}(n, q)$.

TWIERDZENIE 4.2. (a) *Dla ciągu* Π_n, $n = 0, 1, \ldots$, *mamy*

$$w(n, k) = s(n, n-k), \qquad W(n, k) = S(n, n-k),$$

$$\chi_{\Pi_n}(x) = [x]_n.$$

(b) *Dla ciągu* $\mathscr{P}_n$, $n = 0, 1, \ldots$ *mamy*

$$w(n, k) = (-1)^k \binom{n}{k}, \qquad W(n, k) = \binom{n}{k},$$

$$\chi_{\mathscr{P}_n}(x) = (x-1)^n.$$

(c) *Dla ciągu* $\mathscr{L}(n, q)$, $n = 0, 1, \ldots$ *mamy*

$$w(n, k) = (-1)^k q^{\binom{k}{2}} \binom{n}{k}_q, \qquad W(n, k) = \binom{n}{k}_q,$$

$$\chi_{\mathscr{L}(n,q)}(x) = \prod_{i=0}^{n-1} (x-q^i).$$

Dowód. Część (a) została już wykazana.

(b) Korzystając z twierdzenia 3.7 mamy

$$w(n, k) = \sum_{a:\,|a|=k} \mu(\emptyset, a) = (-1)^k \binom{n}{k},$$

równość $W(n, b) = \binom{n}{k}$ zaś nie wymaga komentarza.

$$\chi_{\mathscr{P}_n}(x) = \sum_{k=0}^{n} w(n, n-b)\, x^{n-k} = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^k = (x-1)^n.$$

(c) Zgodnie z twierdzeniem 3.11

$$w(n, k) = \sum_{T:\, \dim T = k} \mu(0, T) = (-1)^k q^{\binom{k}{2}} \binom{n}{k}_q.$$

Oczywiście $W(n, k) = \binom{n}{k}_q$, żądany wzór na $\chi_{\mathscr{L}(n,q)}(x)$ otrzymujemy natomiast z tożsamości (3.13). □

Wyznaczone w tym twierdzeniu wartości współczynników pierwszego i drugiego rodzaju możemy teraz podstawić do twierdzenia 4.1.

WNIOSEK 4.3.

(a)
$$b_n = \sum_{k=0}^{n} S(n, k)\, a_k, \quad n = 0, 1, \ldots, \Leftrightarrow$$
$$\Leftrightarrow a_n = \sum_{k=0}^{n} s(n, k)\, b_k, \quad n = 0, 1, \ldots,$$

(b)
$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k, \quad n = 0, 1, \ldots, \Leftrightarrow$$
$$\Leftrightarrow a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k, \quad n = 0, 1, \ldots,$$

(c)
$$b_n = \sum_{k=0}^{n} \binom{n}{k}_q a_k, \quad n = 0, 1, \ldots, \Leftrightarrow$$
$$\Leftrightarrow a_n = \sum_{k=0}^{n} (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{k}_q b_k, \quad n = 0, 1, \ldots$$

Wyrazy ciągów $a_0, a_1, \ldots$ *oraz* $b_0, b_1, \ldots$ *mogą być elementami dowolnego pierścienia charakterystyki zero.*

Dowód. (b) Mamy $w(n, n-k) = (-1)^{n-k}\binom{n}{n-k} = (-1)^{n-k}\binom{n}{k}$, $W(n, n-k) = \binom{n}{n-k} = \binom{n}{k}$.

(c) $w(n, n-k) = (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{n-k}_q = (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{k}_q$, $W(n, n-k) = \binom{n}{n-k}_q = \binom{n}{k}_q$. □

Dla przykładu zastosujemy wniosek 4.3 do wyznaczenia liczby nieporządków (por. tw. 1.7.4). Liczba permutacji $\varphi \in S_n$ ustalających dokładnie $n-k$ elementów jest równa oczywiście $\binom{n}{k} D_k$, gdzie D_k jest liczbą nieporządków na zbiorze k-elementowym. Mamy
$$n! = \sum_{k=0}^{n} \binom{n}{k} D_k \quad (D_0 = 1),$$
a więc zgodnie z wnioskiem 4.3 (b)
$$D_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k!.$$

Jako jeszcze jedno zastosowanie wniosku 4.3 podamy teraz wzór na liczbę podzbiorów rozpinających przestrzeń $V(n, q)$. Dla dowolnego $k \geqslant 0$ oznaczmy przez a_k liczbę tych podzbiorów $A \subseteq V(k, q)$, które rozpinają całą przestrzeń $V(k, q)$. Skoro każdy niepusty podzbiór przestrzeni $V(n, q)$ rozpina pewną podprzestrzeń, to

$$2^{q^n}-1 = \sum_{k=0}^{n} \binom{n}{k}_q a_k$$

(przyjmujemy, że zbiór pusty nie rozpina żadnej podprzestrzeni). Zgodnie z wnioskiem 4.3 (c) mamy

TWIERDZENIE 4.4. *Liczba podzbiorów rozpinających przestrzeń $V(n, q)$ jest równa*

$$a_n = \sum_{k=0}^{n} (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{k}_q (2^{q^k}-1) = \sum_{k=0}^{n} (-1)^k q^{\binom{k}{2}} \binom{n}{k}_q (2^{q^{n-k}}-1). \qquad \square$$

§ 5. Zastosowania wzorów inwersyjnych

Pokażemy najpierw, że wzór inwersyjny w przypadku zbioru $\mathscr{P}(X)$ daje klasyczną zasadę włączania–wyłączania (p. § 1.7). Niech $P_1, \ldots, P_n$ będzie ciągiem podzbiorów zbioru skończonego S. Załóżmy, że dana jest funkcja rzeczywista $v\colon S \to \boldsymbol{R}$. Przyjmijmy oznaczenie

$$v(T) = \sum_{a \in T} v(a) \qquad \text{dla dowolnego } T \subseteq S.$$

$v(T)$ będziemy nazywali *wagą* zbioru T. Niech $X = \{1, \ldots, n\}$. Dla dowolnego $Y \subseteq X$ oznaczmy przez $F_=(Y)$ wagę zbioru tych elementów, które należą do podzbiorów P_i, $i \in Y$, i tylko do tych podzbiorów, tzn.

$$F_=(Y) = v\Big(\bigcap_{i \in Y} P_i \cap \bigcap_{j \in X \setminus Y} (S \setminus P_j)\Big)$$

(zauważmy, że jest to waga pewnej składowej rodziny $\{P_1, \ldots, P_n\}$). Przez $F_\geqslant(Y)$ oznaczmy wagę zbioru tych elementów, które należą do podzbiorów P_i, $i \in Y$, i – być może – pewnych innych podzbiorów P_i:

$$F_\geqslant(Y) = v\Big(\bigcap_{i \in Y} P_i\Big).$$

Korzystając z faktu, iż $v(Z \cup T) = v(Z) + v(T)$ dla $Z \cap T = \emptyset$, łatwo otrzymujemy

$$F_\geqslant(Y) = \sum_{Z\colon Z \supseteq Y} F_=(Z).$$

Na mocy wzoru inwersyjnego (twierdzenie 2.2) mamy więc

(5.1) $$F_=(Y) = \sum_{Z\colon Z \supseteq Y} \mu(Y, Z) F_\geqslant(Z) = \sum_{Z\colon Z \supseteq Y} (-1)^{|Z|-|Y|} v\Big(\bigcap_{i \in Z} P_i\Big).$$

W szczególności

(5.2)
$$F_=(\emptyset) = \nu\Big(\bigcap_{j\in X} (S\setminus P_j)\Big) = \nu(S)-\nu\Big(\bigcup_{j\in X} P_i\Big) = \\ = \sum_{Z:\, Z\subseteq X} (-1)^{|Z|}\nu\Big(\bigcap_{i\in Z} P_i\Big),$$

a stąd, po uwzględnieniu faktu, iż $\bigcap_{i\in Z} P_i = S$ dla $Z=\emptyset$ otrzymujemy

TWIERDZENIE 5.1 (Sylvester).
$$\nu\Big(\bigcup_{j=1}^{n} P_i\Big) = \sum_{i=1}^{n} \nu(P_i) - \sum_{1\le i<j\le n} \nu(P_i\cap P_j) + \sum_{1\le i<j<k\le n} \nu(P_i\cap P_j\cap P_k) - \\ \ldots + (-1)^{n-1}\nu\Big(\bigcap_{i=1}^{n} P_i\Big). \quad \square$$

Najczęściej w zastosowaniach mamy do czynienia z sytuacją, gdy $\nu(a)=1$ dla każdego $a\in S$, i w konsekwencji $\nu(Y)=|Y|$.

Udowodnimy teraz ogólniejszą wersję zasady włączania–wyłączania. W tym celu oznaczmy przez ν_k wagę zbioru tych elementów w S, które należą do dokładnie k spośród zbiorów P_i. Mamy wtedy, zgodnie z (5.1),
$$\nu_k = \sum_{\substack{Y:\, Y\subseteq X\\ |Y|=k}} F_=(Y) = \sum_{\substack{Y:\, Y\subseteq X\\ |Y|=k}} \sum_{Z:\, Z\supseteq Y} (-1)^{|Z|-k}\nu\Big(\bigcap_{i\in Z} P_i\Big) = \\ = \sum_{Z:\, |Z|\ge k} \sum_{\substack{Y:\, Y\subseteq Z\\ |Y|=k}} (-1)^{|Z|-k}\nu\Big(\bigcap_{i\in Z} P_i\Big).$$

Otrzymujemy stąd ostatecznie

TWIERDZENIE 5.2 (Jordan). *Waga zbioru elementów należących do dokładnie k spośród zbiorów $P_1, \ldots, P_n$ jest równa*
$$\nu_k = \sum_{m=k}^{n} (-1)^{m-k}\binom{m}{k} \sum_{\substack{Z:\, Z\subseteq X\\ |Z|=m}} \nu\Big(\bigcap_{i\in Z} P_i\Big). \quad \square$$

Niektóre zastosowania zasady włączania–wyłączania poznaliśmy już w § 1.7. Podamy teraz dalsze przykłady.

Liczba macierzy zerojedynkowych bez linii zerowych. Będziemy rozważali macierze zerojedynkowe o n wierszach i m kolumnach, zawierające dokładnie k jedynek. Ponumerujmy wiersze liczbami $1, \ldots, n$, kolumny zaś liczbami $n+1, \ldots, n+m$, i oznaczmy $W=\{1,\ldots,n\}$, $K=\{n+1,\ldots,n+m\}$, $L=W\cup K$. Dla dowolnego $i\in L$ niech P_i będzie zbiorem tych macierzy, które mają same zera w linii (tzn. wierszu lub kolumnie) o numerze i. Łatwo zauważyć, że dla dowolnego $Z\subseteq L$
$$F_{\ge}(Z) = \Big|\bigcap_{i\in Z} P_i\Big| = \binom{|W\setminus Z|\cdot|K\setminus Z|}{k}.$$

Zgodnie ze wzorem (5.2) liczba macierzy bez linii zerowych wyraża się wzorem

(5.3)
$$F_{=}(\emptyset) = \sum_{Z:\, Z \subseteq L} (-1)^{|Z|} \binom{|W \setminus Z| \cdot |K \setminus Z|}{k} =$$
$$= \sum_{A:\, A \subseteq W} \sum_{B:\, B \subseteq K} (-1)^{|A|+|B|} \binom{(n-|A|)(m-|B|)}{k} =$$
$$= \sum_{i=0}^{n} \sum_{j=0}^{m} (-1)^{i+j} \binom{n}{i}\binom{m}{j}\binom{(n-i)(m-j)}{k} =$$
$$= \sum_{i=0}^{n} \sum_{j=0}^{m} (-1)^{n+m-i-j} \binom{n}{i}\binom{m}{j}\binom{ij}{k}$$

(ostatnia równość powstaje przez zamianę i na $n-i$ oraz j na $m-j$).

Problem Lucasa (*problème des ménages*). Zbadamy, iloma sposobami można rozsadzić przy okrągłym stole n par małżeńskich tak, by

(a) kobiety i mężczyźni siedzieli na przemian,

(b) żadna żona nie siedziała obok swego męża.

Mamy zatem $2n$ miejsc przy okrągłym stole i możemy rozsadzić mężczyzn dowolnie na miejscach $1, 3, \ldots, 2n-1$. Kobiety zajmują miejsca $2, 4, \ldots, 2n$. Zauważmy, że cykliczne przestawienie wszystkich osób nie zmienia istotnie konfiguracji. Mężczyzn możemy zatem rozsadzić $(n-1)!$ sposobami (bo cykliczne przesunięcie „zlepia” n permutacji). Jest oczywiste, że każde rozsadzenie mężczyzn generuje tyle samo rozsadzeń kobiet. Wystarczy więc jeśli znajdziemy liczbę U_n rozsadzeń (spełniających warunki (a), (b)) dla ustalonego rozmieszczenia mężczyzn; liczbę wszystkich rozwiązań otrzymamy jako $(n-1)!\, U_n$. Załóżmy, że mężczyzna o numerze i zajmuje miejsce $2i-1$ ($i = 1, \ldots, n$). Dla jego żony, tzn. kobiety o numerze i, „zabronione” są miejsca o numerach $2i-2$, $2i$, jeśli $i > 1$, oraz $2n$, 2, jeśli $i = 1$. Niech P_1 oznacza zbiór tych permutacji φ zbioru $\{1, \ldots, n\}$, dla których $\varphi(1) = 1$, P_2 zbiór tych permutacji, dla których $\varphi(1) = 2$, P_3 zbiór tych permutacji, dla których $\varphi(2) = 2$ itd. Ogólnie

$$P_{2j-1} = \{\varphi\colon\ \varphi(j) = j\}, \qquad 1 \leqslant j \leqslant n,$$
$$P_{2j} = \{\varphi\colon\ \varphi(j) = j+1\}, \qquad 1 \leqslant j < n,$$
$$P_{2n} = \{\varphi\colon\ \varphi(n) = 1\}.$$

Dla zastosowania zasady włączania–wyłączania należy wyznaczyć liczność przecięcia $P_{i_1} \cap \ldots \cap P_{i_k}$ dla dowolnego k i dowolnego ciągu wskaźników $i_1 < \ldots < i_k$.

Udowodnimy teraz, że

$$|P_{i_1} \cap \ldots \cap P_{i_k}| = \begin{cases} 0, & \text{jeśli zbiór } \{i_1, \ldots, i_k\} \text{ zawiera kolejne liczby,} \\ & \text{bądź też liczby } 2n \text{ i } 1, \\ (n-k)! & \text{w przeciwnym przypadku.} \end{cases}$$

Istotnie, jeśli $\varphi \in P_{2j-1} \cap P_{2j}$, $j < n$, to z jednej strony $\varphi(j) = j$, z drugiej zaś $\varphi(j) = j+1$. Sprzeczność otrzymujemy również, jeśli założymy $\varphi \in P_{2j} \cap P_{2j+1}$, $j < n$. Wtedy bowiem $\varphi(j) = j+1$ i $\varphi(j+1) = j+1$. Podobnie jest w przypadku, gdy jeden ze wskaźników równy jest $2n$, drugi zaś 1 lub $2n-1$. Załóżmy teraz, że zbiór $\{i_1, \ldots, i_k\}$ nie zawiera pary kolejnych liczb, ani też pary $\{1, 2n\}$. Wtedy oczywiście $k \leqslant n$, i k ustalonych wartości dla φ może być uzupełnionych na $(n-k)!$ sposobów.

W myśl zasady włączania–wyłączania otrzymujemy

$$U_n = \sum_{Z:\, Z \subseteq \{1, \ldots, 2n\}} (-1)^{|Z|} \Big|\bigcap_{i \in Z} P_i\Big| = \sum_{k=0}^{n} (-1)^k g(2n, k)(n-k)!, \tag{5.4}$$

gdzie $g(n, k)$ oznacza liczbę tych podzbiorów k-elementowych zbioru $\{1, \ldots, n\}$, które nie zawierają dwóch kolejnych liczb, an też pary $\{1, n\}$.

Lemat 5.3 (Kaplansky [1]). *Dla* $k \leqslant \lfloor n/2 \rfloor$

$$g(n, k) = \frac{n}{n-k} \binom{n-k}{k}. \tag{5.5}$$

Dowód. Oznaczmy przez $f(n, k)$ liczbę tych podzbiorów k-elementowych zbioru $\{1, \ldots, n\}$, które nie zawierają dwóch kolejnych liczb. Łatwo wykazać, że

$$f(n, k) = \binom{n-k+1}{k}, \qquad k \leqslant \lfloor (n+1)/2 \rfloor \tag{5.6}$$

(p. zad. 1.45). Rozważmy teraz dowolny podzbiór k-elementowy nie zawierający żadnej z par $\{i, i+1\}$, $1 \leqslant i < n$, ani $\{1, n\}$. Jeśli n należy do naszego podzbioru, to nie zawiera on liczb $n-1$ i 1, pozostałe $k-1$ elementów możemy zatem wybrać $f(n-3, k-1)$ sposobami. Podobnie, zbiorów nie zawierających liczby n jest $f(n-1, k)$. Stąd

$$g(n, k) = f(n-3, k-1) + f(n-1, k) = \binom{n-k-1}{k-1} + \binom{n-k}{k} =$$

$$= \left(\frac{k}{n-k} + 1\right)\binom{n-k}{k} = \frac{n}{n-k}\binom{n-k}{k}.$$

Podstawiając wartość $g(2n, k)$ do (5.4) otrzymujemy ostatecznie

Twierdzenie 5.4 (Touchard [1]).

$$U_n = \sum_{k=0}^{n} (-1)^k \frac{2n}{2n-k} \binom{2n-k}{k}. \;\square \tag{5.7}$$

Sito Eratostenesa. Niech $p_1, p_2, \ldots$ będzie ciągiem kolejnych liczb pierwszych. Dla dowolnego rzeczywistego $x > 0$ oznaczmy przez $\pi(x)$ ilość liczb pierwszych nie przekraczających x, tzn. $\pi(x) = \max\{i:\ p_i \leqslant x\}$. Niech

$$S = \{2, 3, \ldots, n\}, \qquad P_i = \{m \in S:\ p_i | m\}$$

dla $1 \leqslant i \leqslant k = \pi(\sqrt{x})$. Dla dowolnego ciągu wskaźników $i_1 < \ldots < i_r$ mamy

$$|P_{i_1} \cap \ldots \cap P_{i_r}| = \left\lfloor \frac{n}{p_{i_1} \cdots p_{i_r}} \right\rfloor,$$

jako że $P_{i_1} \cap \ldots \cap P_{i_r}$ jest zbiorem liczb w S podzielnych przez $p_{i_1} \ldots p_{i_r}$. Biorąc pod uwagę fakt, że $S \setminus \bigcup_{i=1}^{k} P_i$ jest zbiorem liczb pierwszych p takich, że $\sqrt{n} < p \leqslant n$, otrzymujemy z zasady włączania–wyłączania

TWIERDZENIE 5.5.

$$\pi(n) - \pi(\sqrt{n}) = n - 1 - \sum_{1 \leqslant i \leqslant k} \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{1 \leqslant i < j \leqslant k} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \ldots + (-1)^k \left\lfloor \frac{n}{p_1 p_2 \cdots p_k} \right\rfloor, \tag{5.8}$$

gdzie $k = \pi(\sqrt{n})$. □

Zobaczmy teraz jak wygląda twierdzenie inwersyjne w przypadku zbioru $\langle \boldsymbol{N}, | \rangle$:

Jeśli

$$F_{\leqslant}(n) = \sum_{d:\, d|n} F_{=}(d), \tag{5.9}$$

to

$$F_{=}(n) = \sum_{d:\, d|n} F_{\leqslant}(d)\,\mu(d, n). \tag{5.10}$$

Zgodnie z twierdzeniem 3.8 $\mu(d, n)$ zależy tylko od ilorazu n/d. Możemy więc (5.10) zapisać jako

$$F_{=}(n) = \sum_{d:\, d|n} F_{\leqslant}(d)\,\mu\left(\frac{n}{d}\right) = \sum_{d:\, d|n} F_{\leqslant}\left(\frac{n}{d}\right)\mu(d), \tag{5.11}$$

gdzie μ oznacza tym razem klasyczną teorioliczbową funkcję Möbiusa (jednego argumentu) określoną wzorem

$$\mu(m) = \begin{cases} (-1)^k, & \text{jeśli } m \text{ jest iloczynem } k \text{ różnych liczb pierwszych,} \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Czytelnik bez trudu sprawdzi, że

$$\mu(m) = \mu_{\boldsymbol{P}}(n, m \cdot n),$$

gdzie $\boldsymbol{P}$ jest zbiorem liczb naturalnych z relacją podzielności, n zaś dowolną liczbą naturalną. Ta właśnie zależność stała się podstawą do rozwiniętej w tym rozdziale teorii.

Oto kilka zastosowań wzoru (5.11).

Funkcja φ Eulera. Określamy ją następująco:

$$\varphi(n) = \{k\colon\ 1 \leqslant k \leqslant n \wedge (n, k) = 1\},$$

tzn. $\varphi(n)$ jest ilością liczb naturalnych nie przekraczających n i względnie pierwszych z n. Zauważmy, że zbiór $S = \{1, \ldots, m\}$ możemy podzielić na podzbiory rozłączne

$$S_d = \{k \in S\colon\ (n, k) = d\}, \qquad d|n.$$

Mamy oczywiście

$$|S| = n = \sum_{d:\, d|n} |S_d|.$$

Lecz $|S_d| = \varphi(n/d)$, gdyż

$$(n, k) = d \Leftrightarrow (n/d, k) = 1.$$

Otrzymujemy zatem równość

$$n = \sum_{d:\, d|n} \varphi(n/d) = \sum_{e:\, e|n} \varphi(e),$$

i zgodnie ze wzorem inwersyjnym (5.11)

$$\varphi(n) = \sum_{d:\, d|n} d\mu\left(\frac{n}{d}\right) = \sum_{d:\, d|n} \mu(d)\frac{n}{d} = \tag{5.12}$$

$$= n\left(1 - \sum_{i:\, 1 \leqslant i \leqslant m} \frac{1}{q_i} + \sum_{i,j:\, 1 \leqslant i < j \leqslant m} \frac{1}{q_i q_j} - \ldots + (-1)^m \frac{1}{q_1 \ldots q_m}\right),$$

gdzie $q_1, \ldots, q_m$ są wszystkimi dzielnikami pierwszymi liczby n. Zauważmy, że wyrażenie w nawiasie jest równe $\prod_{i=1}^{m} (1 - 1/q_i)$. Otrzymujemy więc ostatecznie

TWIERDZENIE 5.6. *Funkcja φ Eulera wyraża się wzorem*

$$\varphi(n) = n \prod_{p} (1 - 1/p),$$

gdzie p przebiega wszystkie dzielniki pierwsze liczby n. □

Warto zauważyć, że twierdzenie to można też udowodnić posługując się zasadą włączania–wyłączania. Wystarczy w tym celu przyjąć

$$S = \{1, \ldots, n\}, \qquad P_i = \{m \in S\colon\ q_i|m\}, \qquad 1 \leqslant i \leqslant k.$$

Wtedy $\varphi(n)$ jest liczbą elementów zbioru S nie należących do żadnego ze zbiorów P_i, i wzór (5.12) otrzymujemy ze wzoru Sylvestera, jeśli zauważymy, że

$$|P_{i_1} \cap \ldots \cap P_{i_k}| = \frac{n}{q_{i_1} \ldots q_{i_k}}.$$

Jest to sytuacja dość typowa – często rezultaty otrzymane przez inwersję w różnych zbiorach częściowo uporządkowanych możemy również otrzymać stosując klasyczną zasadę włączania–wyłączania. Jednakże użycie tej zasady nie zawsze jest tak przejrzyste jak skorzystanie ze wzorów inwersyjnych dla zbioru częściowo uporządkowanego zwykle w naturalny sposób wyznaczonego przez rozwiązywany problem.

Problem naszyjników (*liczba słów cyklicznych*). Załóżmy, że mamy do dyspozycji koraliki w k kolorach, przy czym liczba koralików każdego koloru jest nieograniczona.

Zadaniem naszym będzie obliczenie, iloma sposobami możemy z tych koralików sporządzić naszyjnik długości n. Zauważmy przede wszystkim, że każdy taki naszyjnik możemy zakodować przez ciąg $\langle k_0, \ldots, k_{n-1}\rangle$, gdzie $k_i \in \{1, \ldots, k\}$ dla $0 \leqslant i \leqslant n-1$. Ciąg ten opisuje naszyjnik powstały przez nanizanie kolejno na nitkę koralików koloru $k_0, k_1, \ldots, k_{n-1}$ a następnie związanie nitki. Oczywiście ciąg powstały z $\langle k_0, \ldots, k_{n-1}\rangle$ przez cykliczne przesunięcie – tzn. każdy ciąg postaci $\langle k_p, k_{p+1}, \ldots, k_{p+n-1}\rangle$, gdzie wskaźniki obliczamy modulo n – opisuje ten sam naszyjnik. W zbiorze wszystkich k^n ciągów $\langle k_0, \ldots, k_{n-1}\rangle$ mamy więc relację równoważności zdefiniowaną następująco: dwa ciągi są równoważne, jeśli jeden powstaje z drugiego przez przesunięcie cykliczne. Naszym zadaniem jest znalezienie liczby klas abstrakcji tej relacji (ściśle rzecz biorąc, uprościliśmy nieco zagadnienie, gdyż nie założyliśmy, że ciągi $\langle k_0, k_1, \ldots, k_{n-1}\rangle$ oraz $\langle k_{n-1}, k_{n-2}, \ldots, k_0\rangle$ reprezentują ten sam naszyjnik – należałoby więc mówić raczej o liczbie słów cyklicznych, a nie o liczbie naszyjników).

Przez *okres* ciągu $\langle k_0, \ldots, k_{n-1}\rangle$ rozumiemy najmniejszą dodatnią liczbę pozycji, o którą należy cyklicznie przesunąć ten ciąg tak, by przeszedł on na siebie, tzn. najmniejszą liczbę $p > 0$ taką, że $\langle k_0, \ldots, k_{n-1}\rangle = \langle k_p, \ldots, k_{n-1+p}\rangle$ (wskaźniki obliczamy modulo n).

Zauważmy, że okres ciągu jest dzielnikiem jego długości. Istotnie, przypuśćmy, że d jest okresem ciągu $\langle k_0, \ldots, k_{n-1}\rangle$ i $d \nmid n$, tzn. $r = (d, n) < d$. Na mocy algorytmu Euklidesa (p. Dodatek A) istnieje wtedy d całkowite takie, że $ad \equiv r (\mathrm{mod}\ n)$, a więc efekt cyklicznego przesunięcia rozważanego ciągu o ad pozycji i r pozycji jest ten sam. Jednakże przy przesunięciu o ad pozycji (wielokrotność okresu) ciąg przechodzi na siebie, przy przesunięciu zaś o r pozycji ciąg nie przechodzi na siebie, gdyż $1 \leqslant r < d$. Musi więc być $d|n$.

Oznaczmy przez C_d liczbę ciągów długości n o okresie d. Wszystkich ciągów długości n jest k^n, zatem

$$k^n = \sum_{d:\, d|n} C_d,$$

i na mocy wzoru inwersyjnego

$$C_d = \sum_{e:\, e|d} \mu\left(\frac{d}{e}\right) k^e.$$

Łatwo zauważyć, że klasa abstrakcji zawierająca ciąg o okresie d składa się z d różnych przesunięć cyklicznych tego ciągu. Tak więc szukana liczba naszyjników jest równa

$$S_n = \sum_{d:\, d|n} \frac{1}{d} C_d = \sum_{d:\, d|n} \frac{1}{d} \sum_{e:\, e|d} \mu\left(\frac{d}{e}\right) k^e.$$

Zmieniając porządek sumowania i stosując podstawienie $q = d/e$ mamy

$$S_n = \sum_{e:\, e|n} \sum_{q:\, q|(n/e)} \frac{1}{qe} \mu(q) k^e.$$

Jeśli teraz zauważymy, że zgodnie z wzorem (5.12)

$$\sum_{q:\, q|(n/e)} \frac{1}{qe} \mu(q) = \frac{1}{n} \sum_{q:\, q|(n/e)} \frac{n/e}{q} \mu(q) = \frac{1}{n} \varphi\left(\frac{n}{e}\right),$$

to ostatecznie otrzymujemy

TWIERDZENIE 5.7. *Liczba słów cyklicznych długości n jest równa*

$$S_n = \frac{1}{n} \sum_{d:\, d|n} \varphi\left(\frac{n}{d}\right) k^d. \quad \square$$

Liczba grafów spójnych. Na zakończenie podamy przykład zastosowania twierdzenia inwersyjnego dla kraty podziałów zbioru. Wyznaczymy liczbę grafów spójnych o ustalonym, n-elementowym zbiorze wierzchołków X. Zauważmy, że dowolny graf indukuje podział swojego zbioru wierzchołków na bloki będące zbiorami wierzchołków składowych spójnych tego grafu. Dla dowolnego podziału $\pi \in \Pi(X)$ oznaczmy przez $F_=(\pi)$ liczbę grafów indukujących podział π, i niech

$$F_{\leqslant}(\pi) = \sum_{\sigma:\, \sigma \leqslant \pi} F_=(\sigma).$$

Wobec wzoru inwersyjnego liczba grafów spójnych jest równa

$$F_=(1) = \sum_{\pi \in \Pi(X)} \mu(\pi, 1) F_{\leqslant}(\pi). \tag{5.13}$$

Jeśli π jest typu $\lambda = \langle \lambda_1, \ldots, \lambda_n \rangle$, tzn. jeśli zawiera λ_i bloków i-elementowych, $i = 1, \ldots, n$, to łatwo zauważyć, że

$$F_{\leqslant}(\pi) = \prod_{i=1}^{n} 2^{\binom{i}{2}\lambda_i}.$$

Z kolei z twierdzenia 3.10 otrzymujemy

$$\mu(\pi, 1) = (-1)^{|\pi|-1} (|\pi|-1)! = (-1)^{|\lambda|-1} (|\lambda|-1)!,$$

gdzie $|\lambda| = \sum_{i=1}^{n} \lambda_i$. Jeśli jeszcze uwzględnimy, że liczba podziałów typu λ jest równa

$$\frac{n!}{\prod_{i=1}^{n} \lambda_i!(i!)^{\lambda_i}},$$

(p. tw. 1.8.2), to z (5.13) otrzymamy

TWIERDZENIE 5.8. *Liczba grafów spójnych o ustalonym n-elementowym zbiorze wierzchołków jest równa*

$$G_n = n! \sum_{\lambda: \sum_i i\lambda_i = n} (-1)^{|\lambda|-1}(|\lambda|-1)! \prod_{i=1}^{n} \frac{2^{\binom{i}{2}\lambda_i}}{\lambda_i!(i!)^{\lambda_i}}. \quad \square$$

Zadania

1. Uzupełnić dowód twierdzenia 1.1.

2. Udowodnić, że algebra $\mathscr{A}(P)$ jest przemienna wtedy i tylko wtedy, gdy P jest antyłańcuchem.

3. Udowodnić, że każdy lokalnie skończony porządek częściowy na zbiorze co najwyżej przeliczalnym można rozszerzyć do lokalnie skończonego porządku liniowego.

4. Udowodnić, że jeśli odcinki $[x, y]$ i $[z, t]$ są izomorficzne, to $\mu(x, y) = \mu(z, t)$.

5. Wykazać, że operator różnicowy D jest prawostronną odwrotnością operatora sumacyjnego S, tzn. że (2.8) pociąga za sobą (2.7).

6. Wykazać, że

(a) $\zeta^2(x, y) = |[x, y]|$,

(b) $2\delta - \zeta$ ma odwrotność i $(2\delta-\zeta)^{-1}(x, y)$ jest równe liczbie wszystkich łańcuchów o początku w x i końcu w y.

7. Wykazać, że jeśli y jest bezpośrednim następnikiem elementu x, to $\mu(x, y) = -1$.

8. Wskazać przykład iloczynu skończonych porządków częściowych, który nie jest lokalnie skończony.

9. Wykazać twierdzenie 3.10 korzystając z twierdzenia Weisnera (twierdzenie 3.5).

10. Wykazać, że $\chi_{P_1 \times P_2}(x) = \chi_{P_1}(x) \cdot \chi_{P_2}(x)$.

11. Wykazać, że każdy porządek częściowy P mający elementy: najmniejszy 0 i największy 1 spełnia

$$w_P(0) = 1, \quad w_P(1) = -W_P(1), \quad w_P(r(1)) = \mu_P(0, 1).$$

12. *Liczbą Laha* $L(n, k)$, $n \geqslant k \geqslant 1$, *nazywamy liczbę*

$$L(n, k) = (-1)^n \frac{n!}{k!}\binom{n-1}{k-1}.$$

Wykazać następującą własność inwersyjną dla liczb Laha:
Jeśli $\langle a_n \rangle_{n=1}^{\infty}$, $\langle b_n \rangle_{n=1}^{\infty}$ spełniają warunki

$$b_n = \sum_{k=1}^{n} L(n, k) a_k, \quad n = 1, 2, \ldots,$$

to

$$a_n = \sum_{k=1}^{n} L(n, k) b_k, \qquad n = 1, 2, \ldots$$

13. Wyznaczyć wzór na s_{nm} (liczbę funkcji z X na Y, gdzie $|X| = n$, $|Y| = m$) korzystając z zależności

$$m^n = \sum_{k=0}^{m} \binom{m}{k} s_{nk}$$

oraz twierdzenia 4.1.

14. Wykazać, że $(n-2)U_n = n(n-2)U_{n-1} + nU_{n-2} + 4(-1)^{k+1}$.

15. Wykazać, że $\lim_{n\to\infty} \frac{U_n}{n!} = e^{-2}$.

16. (a) Wykazać, że istnieje dokładnie jedna funkcja Λ spełniająca warunek

$$\sum_{d:\, d|n} \Lambda(d) = \ln n.$$

(b) Wykazać, że

$$\Lambda(n) = \begin{cases} \ln p, & \text{jeśli } n = p^k \text{ dla pewnego } k, \\ 0 & \text{w przeciwnym przypadku.} \end{cases}$$

17. Wykazać, że $\pi(n) - \pi(\sqrt{n}) = -1 + \sum_{d=1}^{n} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor$.

ROZDZIAŁ 3

FUNKCJE TWORZĄCE

W niniejszym rozdziale powracamy do funkcji tworzących, pojęcia niezwykle przydatnego w kombinatorycznych problemach zliczania. W odróżnieniu od „analitycznego” podejścia z § 10 pierwszego rozdziału, funkcje tworzące traktujemy tu jako szeregi formalne, będące w istocie jedynie wygodną reprezentacją formalną ciągu współczynników szeregu. Przy takim „algebraicznym” podejściu odpada konieczność badania zbieżności rozpatrywanych szeregów, co więcej, szeregi rozbieżne w sensie analitycznym stają się „legalnymi” obiektami rozważań. Pokazujemy tu związek funkcji tworzących różnych typów — takich jak na przykład funkcja tworząca eksponencjalna znana z § 10 pierwszego rozdziału — z algebrami incydencji odpowiednich zbiorów częściowo uporządkowanych (por. rozdział 2). Bardzo pożyteczne okazują się w teorii funkcji tworzących, szczególnie przy dowodzeniu różnego rodzaju tożsamości, metody oparte na rozważaniu odpowiednich operatorów liniowych w przestrzeni liniowej wielomianów. W rozdziale tym opisujemy też wiele konkretnych zastosowań funkcji tworzących do rozwiązywania problemów zliczania.

§ 1. Szeregi formalne

Rozdział ten jest poświęcony kombinatorycznym zastosowaniom pewnej klasy pierścieni, a mianowicie pierścieni szeregów formalnych. Argumentów za szerszym potraktowaniem tej dziedziny dostarczają wyniki tego rozdziału wiążące zredukowaną algebrę incydencji z pierścieniem szeregów formalnych jednej zmiennej, a także szerokie zastosowanie funkcji tworzących, a więc właściwie szeregów formalnych. Uogólnione szeregi formalne są także użyte w rozdz. 6, § 3.

Niech X będzie zbiorem, zwanym dalej *zbiorem zmiennych.* Na początek założymy, że X jest zbiorem skończonym i $X = \{x_1, \ldots, x_k\}$. *Jednomianami* będziemy nazywali elementy zbioru funkcji $M = N_0^X$. Jednomian, który na elemencie x_i przyjmuje wartość m_i, będziemy oznaczali przez $x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$. Liczba m_i będzie też zwana *wykładnikiem* x_i. Na zbiorze M wprowadzimy

mnożenie. *Iloczynem* jednomianów $m', m'' \in M$ jest mianowicie jednomian m, oznaczany przez $m' \cdot m''$, lub po prostu $m' m''$, którego wykładniki dla każdej zmiennej x_i są sumą wykładników jednomianów m' i m''. Innymi słowy:

$$x_1^{m'_1} x_2^{m'_2} \ldots x_k^{m'_k} \cdot x_1^{m''_1} x_2^{m''_2} \ldots x_k^{m''_k} = x_1^{m'_1+m''_1} x_2^{m'_2+m''_2} \ldots x_k^{m'_k+m''_k}.$$

Łatwo sprawdzić, że mnożenie to jest przemienne i łączne oraz że ma ono element neutralny. Jest nim jednomian $x_1^0 x_2^0 \ldots x_k^0$, który będzie też oznaczany przez 1.

Zwróćmy uwagę, że dla dowolnego elementu $m \in M$ istnieje tylko skończona liczba par $\{m', m''\} \subseteq M$ takich, że $m = m' m''$. Wynika to stąd, że żadna wartość jednomianu m' nie może być większa od odpowiedniej wartości jednomianu m. Funkcji o tej własności jest tylko skończona liczba. Podobnie jest dla m''. Łatwo zresztą zauważyć, że jeżeli $m = m' m'' \in M$, to każdy element pary $\{m', m''\}$ wyznacza jednoznacznie drugi jednomian.

Szeregiem formalnym o zmiennych ze zbioru X będziemy nazywali każdą funkcję określoną na zbiorze M i o wartościach w ciele C. Jeżeli w jest taką funkcją, a w_m jest jej wartością na jednomianie $m = x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k} \in M$, to szereg formalny w będziemy zapisywali jako

$$\sum_{m \in M} w_m m = \sum_{m \in M} w_m x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}.$$

Wartości w_m nazywamy *współczynnikami szeregu formalnego*, przy czym w_1 nazywamy jego *wyrazem wolnym*. Zbiór tak zdefiniowanych szeregów formalnych będziemy oznaczali przez $C[\![X]\!]$ lub $C[\![x_1, \ldots, x_k]\!]$. W zbiorze $C[\![X]\!]$ określamy działania dodawania i mnożenia w następujący sposób. Jeżeli $w' = \sum_{m \in M} w'_m m$ i $w'' = \sum_{m \in M} w''_m m$ należą do $C[\![X]\!]$, to

$$w' + w'' = \sum_{m \in M} (w'_m + w''_m) m,$$

$$w' \cdot w'' = \sum_{m \in M} w_m m,$$

gdzie

$$w_m = \sum_{m_1 m_2 = m} w'_{m_1} \cdot w''_{m_2}.$$

Zgodnie z naszą uwagą o skończonej liczbie rozkładów każdego jednomianu, współczynniki iloczynu szeregów formalnych są poprawnie zdefiniowane. Wprowadzony iloczyn szeregów nazywamy *iloczynem Cauchy'ego*; jest on znanym każdemu mnożeniem „jak wielomiany". (Porównaj także uogólnioną definicję z rozdziału 6.)

Wprowadzamy też działanie mnożenia przez element ciała, w następujący sposób:

$$c \sum_{m \in M} w_m m = \sum_{m \in M} (c w_m) m \qquad (c \in C).$$

Przy tak zdefiniowanych działaniach $C[\![X]\!]$ jest algebrą przemienną z jedynką, tzn. przestrzenią liniową nad ciałem C z dodatkowym działaniem – mnożeniem – które jest łączne, przemienne, rozdzielne względem dodawania i spełnia warunek $c(w'w'') = (cw')w''$ dla dowolnych $w', w'' \in C[\![X]\!]$, $c \in C$. W szczególności, jeśli nie interesuje nas działanie mnożenia przez element ciała, $C[\![X]\!]$ możemy traktować jako pierścień przemienny z jedynką. Wykazanie wszystkich tych własności sprowadza się do prostych sprawdzeń rachunkowych.

Jedynką jest szereg o wszystkich współczynnikach równych zeru, poza równym 1 współczynniku przy jednomianie 1. Jedynkę tę będziemy utożsamiali zarówno z $1 \in C$ jak i z $1 \in M$, przy oczywistych włożeniach C i M w $C[\![X]\!]$. Podobna konwencja obowiązuje także dla $0 \in C \subseteq C[\![X]\!]$.

Niech X i Y będą dwoma zbiorami zmiennych. Jeżeli $X \subseteq Y$, to algebra $C[\![X]\!]$ wkłada się w naturalny sposób w algebrę $C[\![Y]\!]$. Każdy jednomian algebry $C[\![X]\!]$ traktujemy mianowicie jako jednomian z $C[\![Y]\!]$, który na wszystkich zmiennych z $Y \setminus X$ przyjmuje wartość zero, i rozszerzamy to włożenie na całą algebrę $C[\![X]\!]$. Włożenie to zachowuje działania. Ciało liczb zespolonych C można przy tym traktować jako algebrę szeregów z pustym zbiorem zmiennych.

Jeżeli zbiór zmiennych X jest zbiorem nieskończonym, to jedyna różnica w definicji $C[\![X]\!]$ polega na tym, że określając zbiór jednomianów M, w miejsce wszystkich funkcji z X w N_0, rozpatrujemy tylko takie funkcje, które przyjmują jedynie skończenie wiele wartości różnych od zera, i te funkcje nazywamy jednomianami.

Z szeregami formalnymi o nieskończonej liczbie zmiennych spotykamy się rozpatrując tzw. *szeregi formalne Dirichleta*, czyli wyrażenia postaci $\sum_{n=1}^{\infty} a_n/n^s$. Algebra nad ciałem C tych szeregów z dodawaniem „po współrzędnych" i z mnożeniem:

$$\left(\sum_{n=1}^{\infty} \frac{a_n}{n^s}\right)\left(\sum_{n=1}^{\infty} \frac{b_n}{n^s}\right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}, \tag{1.1}$$

gdzie

$$c_n = \sum_{i:\, i|n} a_i\, b_{n/i},$$

jest izomorficzna z algebrą szeregów formalnych o nieskończonej liczbie zmiennych. Izomorfizm ten wyznaczony jest jak następuje. Przyjmujemy $(1/p_i)^s = x_i$, gdzie p_i jest i-tą liczbą pierwszą, i tak określone odwzorowanie rozszerzamy do izomorfizmu badanych algebr.

Stopniem jednomianu $m = x_1^{m_1} x_2^{m_2} \dots x_k^{m_k}$ będziemy nazywali sumę $m_1 + \dots + m_k$. Dla danego szeregu w będziemy oznaczali przez w_r szereg jednomianów stopnia r, to znaczy szereg, który ma takie same współczynniki jak szereg w przy jednomianach stopnia r, a pozostałe współczynniki równe zeru. (W przypadku, gdy

liczba zmiennych w szeregu w jest skończona, w_r jest wielomianem jednorodnym stopnia r.) Następujący lemat podaje interesującą własność szeregów w_r.

LEMAT 1.1. *Jeśli* $w = w' w''$, *to*

$$w_r = \sum_{j=0}^{r} w'_j w''_{r-j}.$$

Łatwy dowód pozostawiamy Czytelnikowi. (por. zad. 2). □

Dla szeregu formalnego $w \neq 0$ oznaczmy przez $\omega(w)$ najmniejszą liczbę r taką, że $w_r \neq 0$, oraz przyjmijmy $\omega(0) = \infty$. Z udowodnionego powyżej faktu wynika natychmiast, że $\omega(w' \cdot w'') = \omega(w') + \omega(w'')$, dla $r = \omega(w')$ i $s = \omega(w'')$ mamy bowiem $(w' \cdot w'')_{r+s} = w'_r \cdot w''_s$. To z kolei implikuje, że algebra szeregów formalnych $C[\![x_1, \ldots, x_l]\!]$ jest dziedziną całkowitości (tzn. jest łącznym, przemiennym pierścieniem z jedynką bez dzielników zera).

Niech $\langle w^{(a)} \rangle_{a \in A}$ będzie indeksowaną rodziną elementów algebry $C[\![X]\!]$. Załóżmy przy tym, że dla każdego jednomianu $m \in M$ istnieje tylko skończona liczba elementów $a \in A$ takich, że szereg $w^{(a)}$ ma przy m współczynnik niezerowy. Łatwo zauważyć, że w przypadku gdy zbiór zmiennych X jest zbiorem skończonym, jest to równoważne temu, że dla każdego $r \in N$ mamy $\omega(w^{(a)}) > r$ dla wszystkich, poza skończoną liczbą elementów $a \in A$. Mówimy wtedy, że rodzina $\langle w^{(a)} \rangle_{a \in A}$ jest *sumowalna*.

Łatwo zauważyć, że przy powyższych założeniach suma $s_m = \sum_{a \in A} w_m^{(a)}$, współczynników przy ustalonym jednomianie $m \in M$ jest określona, gdyż zawiera jedynie skończoną liczbę składników niezerowych. Szereg formalny $\sum_{m \in M} s_m m$ nazywamy wtedy *sumą* rodziny $\langle w^{(a)} \rangle_{a \in A}$. Suma ta z definicji nie zależy od porządku sumowania.

Rozważmy teraz dowolną rodzinę $W = \langle W_x \rangle_{x \in X}$ szeregów formalnych z $C[\![Y]\!]$ indeksowaną zbiorem zmiennych algebry $C[\![X]\!]$. Dla każdego jednomianu $m = x_1^{m_1} \ldots x_k^{m_k}$ z $C[\![X]\!]$ określmy

$$m(W) = (W_{x_1})^{m_1} \ldots (W_{x_k})^{m_k}.$$

Oczywiście $m(W)$ jest szeregiem formalnym z $C[\![Y]\!]$. Zauważmy, że jeśli $\omega(W_x) > 0$ dla każdego $x \in X$, to $\omega(m(W)) \geqslant m_1 + \ldots + m_k$ i w konsekwencji — w przypadku gdy zbiór X jest skończony — dla każdego szeregu $w = \sum_{m \in M} w_m m$ z $C[\![X]\!]$ rodzina $\langle w_m m(W) \rangle_{m \in M}$ jest sumowalna. Szereg formalny z $C[\![Y]\!]$ będący jej sumą oznaczamy przez $w(W)$. Intuicyjnie, $w(W)$ otrzymujemy przez podstawienie szeregu $W_x \in C[\![Y]\!]$ w miejsce każdego wystąpienia zmiennej x w szeregu $w \in C[\![X]\!]$.

Opisana powyżej operacja (częściowa) podstawienia zachowuje działania:

$$(w' + w'')(W) = w'(W) + w''(W), \qquad (w' w'')(W) = w'(W)\, w''(W).$$

Co więcej, łatwo sprawdzić, że jeśli $\langle w^{(a)}\rangle_{a\in A}$ jest sumowalną rodziną szeregów z $C[\![X]\!]$, to — zakładając, że X jest skończony i że $\omega(W_x) > 0$ dla każdego $x \in X$ — mamy

$$\Big(\sum_{a\in A} w^{(a)}\Big)(W) = \sum_{a\in A} \big(w^{(a)}(W)\big).$$

Zasadniczym dla zastosowań jest następujące twierdzenie.

TWIERDZENIE 1.2. *Na to, by szereg formalny $w \in C[\![X]\!]$ miał w $C[\![X]\!]$ szereg odwrotny względem mnożenia, potrzeba i wystarcza, by wyraz wolny szeregu w był różny od zera.*

Dowód. Szeregiem odwrotnym dla szeregu $1-x \in C[\![x]\!]$ jest szereg $\sum_{n=0}^{\infty} x^n$, co łatwo sprawdzić przemnażając szeregi. Niech teraz $w \in C[\![X]\!]$ i niech $a \neq 0$ będzie jego wyrazem wolnym. Oznaczmy przez v szereg $1-a^{-1}w \in C[\![X]\!]$. Wówczas $\omega(v) \geqslant 1$, i rodzina $1, v, v^2, \ldots$ jest sumowalna. Podstawiając v w miejsce x we wzorze

$$1 = (1-x)(1+x+x^2+\ldots)$$

otrzymujemy

$$1 = a^{-1}w\cdot(1+v+v^2+\ldots).$$

Zatem szereg w jest odwracalny w $C[\![X]\!]$ i jego odwrotnością jest szereg $a^{-1}(1+v+v^2+\ldots)$.

Konieczność naszego warunku jest oczywista. Jeśli bowiem $\omega(w_1) \neq 0$ lub $\omega(w_2) \neq 0$, to $\omega(w_1 w_2) \neq 0 = \omega(1)$. □

W pierścieniu $C[\![X]\!]$ określamy *pochodną cząstkową* $\partial/\partial x$, gdzie $x \in X$, jako operację liniową na $C[\![X]\!]$ o następujących własnościach: jeżeli $m \in M$ jest jednomianem i wykładnik x w m jest równy 0, to $\partial/\partial x\, m = 0$ i $\partial/\partial x(x^r\cdot m) = rx^{r-1}m$, o ile $r > 0$. Dla szeregu $w = \sum_{m\in M} w_m m \in C[\![X]\!]$ pochodną $\partial/\partial x\, w$ zdefiniujemy jako szereg $\sum_{m\in M} w_m\, \partial/\partial x\, m$. Definicja ta jest poprawna, gdyż jak łatwo stwierdzić, rodzina $\langle \partial w_m m/\partial x\rangle_{m\in M}$ jest sumowalna.

Jeżeli $X = \{x\}$, to oczywiście pochodną $\partial/\partial x$ oznaczamy d/dx, albo D. Mamy wtedy

$$D\Big(\sum_{n=0}^{\infty} a_n x^n\Big) = \sum_{n=0}^{\infty} (n+1)\, a_{n+1} x^n.$$

Zwróćmy uwagę, że chociaż pochodna szeregu formalnego i zwykła pochodna funkcji są czymś całkowicie różnym, to jednak niejednokrotnie udaje się wykazać dla nich analogiczne własności. W szczególności wzory na różniczkowanie iloczynu, ilorazu i pochodną „funkcji złożonej” mają w obydwu przypadkach tę samą postać formalną. Również pozostaje w mocy „rozwinięcie Taylora w punkcie

$x = 0$" (por. zad. 5–9). Ten ostatni wzór bywa użyteczny przy obliczaniu niektórych iloczynów i odwrotności szeregów. Podkreślamy, że „rozwinięcie Taylora w $a \neq 0$" dla szeregów formalnych na ogół nie funkcjonuje. Wynika to stąd, że rodzina $\langle (x-a)^n \rangle_{n \in N}$ nie jest sumowalna dla $a \neq 0$. Paragraf ten zakończymy uwagami na temat związków między szeregami formalnymi jednej zmiennej a funkcjami analitycznymi. Jeśli $\Omega \subseteq C$ jest obszarem zawierającym liczbę 0, to algebra funkcji analitycznych w obszarze Ω jest izomorficzna z podalgebrą algebry szeregów formalnych. Izomorfizmu tego dostarcza rozwinięcie w szereg Taylora funkcji f i utożsamienie rzeczonego rozwinięcia $\sum_{n=0}^{\infty} a_n z^n$ z szeregiem formalnym $\sum_{n=0}^{\infty} a_n x^n$. Stąd wynika, że istnienie odwrotności (względem mnożenia) funkcji analitycznej w obszarze Ω pociąga za sobą istnienie odpowiedniego odwrotnego szeregu formalnego (ale implikacja w drugą stronę nie jest prawdziwa). Łatwo sprawdzić, że izomorfizm ten zachowuje również operację pochodnej. Powyższy fakt pozwala na używanie skrótów. Jeżeli bowiem piszemy $(1-x)^{-1} = \sum_{n=0}^{\infty} x^n$, to mamy na myśli to, że wielomian $1-x$ jest odwrotnością szeregu formalnego $\sum_{n=0}^{\infty} x^n$. Jednakże zapis $e^x = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$ służy jako skrót, który jest poprawny, bowiem, zgodnie z powyższymi uwagami, funkcja analityczna e^x zachowuje się tak jak szereg formalny $\sum_{n=0}^{\infty} \frac{1}{n!} x^n$, i na przykład $De^x = e^x$. Czytelnik powinien mieć cały czas na uwadze, że stosowane w tekście nazwy powszechnie używanych funkcji analitycznych są tylko skrótami nazw szeregów formalnych. Użycie tej konwencji nie prowadzi nas do sprzeczności ze względu na wskazany powyżej izomorfizm.

§ 2. Zredukowana algebra incydencji i funkcje tworzące

Algebra incydencji $\mathscr{A}(\boldsymbol{P})$ zbioru częściowo uporządkowanego $\boldsymbol{P}$ (por. rozdz. 2), choć interesująca z algebraicznego punktu widzenia, jest — dla zastosowań kombinatorycznych — zbyt bogata. Zajmiemy się teraz jej podalgebrą złożoną z tzw. funkcji przesuwalnych. Algebra ta okazuje się izomorficzna z algebrą szeregów formalnych. Dzięki temu będziemy mogli użyć aparatu teorii szeregów formalnych, blisko związanego z analizą matematyczną. Zauważmy najpierw, że relacja $\simeq$ określona w $\boldsymbol{P} \times \boldsymbol{P}$ wzorem

$$\langle x, y \rangle \simeq \langle z, t \rangle \Leftrightarrow \text{odcinek } [x, y] \text{ jest izomorficzny z odcinkiem } [z, t]$$

jest relacją równoważności. Wszystkie pary $\langle x, y \rangle$ takie, że $\neg(x \leqslant y)$, znajdują się w jednej klasie abstrakcji. Podobnie klasę abstrakcji tworzą wszystkie pary $\langle x, x \rangle$ dla $x \in \boldsymbol{P}$.

Będziemy mówili, że funkcja $f \in \mathscr{A}(P)$ jest *przesuwalna* wtedy i tylko wtedy, gdy dla dowolnych x, y, z, t

$$\langle x, y\rangle \simeq \langle z, t\rangle \Rightarrow f(x, y) = f(z, t).$$

Funkcje przesuwalne są to więc funkcje stałe na klasach abstrakcji relacji $\simeq$.

TWIERDZENIE 2.1. *Rodzina funkcji przesuwalnych tworzy podalgebrę algebry $\mathscr{A}(P)$ zamkniętą ze względu na operację odwracania $(\cdot)^{-1}$.*

Dowód. Łatwo stwierdzić, że funkcja stale równa 0 oraz funkcja δ są w naszej podalgebrze. Suma funkcji przesuwalnych jest oczywiście przesuwalna. Dla wykazania zamkniętości ze względu na działanie splotu załóżmy, że φ jest izomorfizmem odcinków $[x, y]$ i $[z, t]$. Zadadniczą własnością, która przyda się też dalej, jest to, że dla dowolnych $u, v \in [x, y]$ mamy $\langle u, v\rangle \simeq \langle \varphi(u), \varphi(v)\rangle$, przy czym funkcją ustalającą izomorfizm jest każdorazowo funkcja φ ograniczona do odpowiedniego zbioru. Niech zatem f i g będą przesuwalne. Wówczas

$$f * g(x, y) = \sum_{x \leqslant z \leqslant y} f(x, z)\cdot g(z, y) = \sum_{x \leqslant z \leqslant y} f\big(\varphi(x), \varphi(z)\big)\cdot g\big(\varphi(z), \varphi(y)\big) =$$
$$= \sum_{z \leqslant v \leqslant t} f(z, v)\cdot g(v, t) = f * g(z, t).$$

Załóżmy teraz, że przesuwalna funkcja f jest odwracalna w algebrze $\mathscr{A}(P)$. Wykażemy przez indukcję, że funkcja odwrotna f^{-1} jest także przesuwalna. Przypomnijmy, że $f^{-1}(x, y) = -(\sum_{x < u \leqslant y} f(x, u)\cdot f^{-1}(u, y))/f(x, x)$. Oczywiście $f(x, x) = f(z, z)$ (bowiem $\langle x, x\rangle \approx \langle z, z\rangle$), a zakładając, że $f^{-1}(u, y) = f^{-1}\big(\varphi(u), \varphi(y)\big)$ dla $x < u \leqslant y$, otrzymujemy

$$f^{-1}(x, y) = -(\sum_{x < u \leqslant y} f(x, u)\, f^{-1}(u, y))/f(x, x) =$$
$$= -\Big(\sum_{x < u \leqslant y} f\big(\varphi(x), \varphi(u)\big)\cdot f^{-1}\big(\varphi(u), \varphi(y)\big)\Big)/f(z, z) =$$
$$= -(\sum_{z < v \leqslant t} f(z, v)\cdot f^{-1}(v, t))/f(z, z) = f^{-1}(z, t). \quad \square$$

Podalgebrę złożoną z funkcji przesuwalnych oznaczamy $\mathscr{R}(P)$. Funkcja ζ jest elementem $\mathscr{R}(P)$, a zatem $\Gamma = \zeta^{-1}$ jest także funkcją przesuwalną. Jeśli α jest typem izomorfizmu odcinka $[x, y]$ (co oznaczamy $\alpha = \overline{[x, y]}$), zaś $z \in [x, y]$, to z wyznacza dwa typy izomorfizmu β i γ jak następuje: β jest typem odcinka $[x, z]$, γ zaś typem odcinka $[z, y]$. W takim przypadku mówimy, że γ *dopełnia* β *do* α. Zazwyczaj element $z \in [x, y]$ taki, że typem $[x, z]$ jest β, nie jest wyznaczony jednoznacznie przez α i β, ani też γ, dopełniające β do α, nie jest wyznaczone przez α i β. Definiujemy zatem liczbę $\left\langle {\alpha \atop \beta, \gamma} \right\rangle$, gdzie $\alpha = \overline{[x, y]}$, jak następuje

$$\left\langle {\alpha \atop \beta, \gamma} \right\rangle = |\{z\colon z \in [x, y] \wedge \overline{[x, z]} = \beta \wedge \overline{[z, y]} = \gamma\}|.$$

Powyższa definicja nie zależy od wyboru reprezentanta $[x, y]$ typu α. Niech $T(\boldsymbol{P})$ będzie rodziną wszystkich typów odcinków w $\boldsymbol{P}$. Każdą funkcję z $\mathscr{R}(\boldsymbol{P})$ możemy identyfikować z odwzorowaniem z $T(\boldsymbol{P})$ w ciało – w naszym przypadku będzie to ciało C. Następne twierdzenie sformułowano używając tej identyfikacji.

Twierdzenie 2.2. *Jeżeli f i g są funkcjami przesuwalnymi, to*

$$f * g(\alpha) = \sum_{\langle\beta,\gamma\rangle} \left\langle {\alpha \atop \beta, \gamma} \right\rangle f(\beta) g(\gamma).$$

Dowód. Wystarczy zauważyć, że jeśli $\overline{[x, y]} = \alpha$, to

$$\sum_{z: x \leqslant z \leqslant y} f(x, z) g(z, y) = \sum_{\langle\beta,\gamma\rangle} \sum_{z \in [x,y]: \overline{[x,z]} = \alpha \wedge \overline{[z,y]} = \beta} f(x, z) g(z, y) =$$

$$= \sum_{\langle\beta,\gamma\rangle} \left\langle {\alpha \atop \beta, \gamma} \right\rangle f(\beta) g(\gamma). \square$$

Szczególnym przypadkiem, dla którego nasza teoria przyjmuje wyjątkowo elegancką postać, jest sytuacja, gdy rozważany porządek częściowy ma tzw. własność dwumianową. Będziemy mówili, że lokalnie skończony zbiór częściowo uporządkowany $\boldsymbol{P} = \langle P, \leqslant \rangle$ ma *własność dwumianową*, jeśli

(1) dla dowolnych $x, y \in P$ każdy łańcuch maksymalny łączący x i y ma tę samą długość, którą oznaczymy $n_{x,y}$ (zauważmy, że jest to warunek Jordana–Dedekinda z § 2, rozdz. 1),

(2) dla każdego $n \in N$ istnieje w $\boldsymbol{P}$ odcinek $[x, y]$ taki, że $n_{x,y} = n$ i każde dwa odcinki o tej własności są izomorficzne.

Wobec powyższego każde dwa odcinki z tą samą i równą n długością łańcuchów maksymalnych mają jednakową ich liczbę. Liczba tą będzie oznaczana przez b_n.

Jeśli s jest łańcuchem maksymalnym łączącym x i y długości $n > 0$ i $1 \leqslant i \leqslant n$, to oczywiście istnieje w łańcuchu s element z taki, że część łańcucha s pomiędzy x i z ma długość i, pozostała zaś część, znajdująca się pomiędzy z i y, ma długość $n-i$ (liczba elementów w łańcuchu jest o jeden większa niż jego długość). Stąd wnioskujemy natychmiast, że liczba elementów $z \in [x, y]$ (gdzie $n_{x,y} = n$) takich, że $n_{x,z} = i$, wynosi $b_n/(b_i \cdot b_{n-i})$. Istotnie, przez każdy taki punkt przechodzi $b_i \cdot b_{n-i}$ łańcuchów maksymalnych, a na mocy naszej poprzedniej uwagi w każdym łańcuchu jest punkt z taki, że $n_{x,z} = i$. Zauważmy jeszcze, że warunki (1) i (2) implikują, że jeśli istnieje typ γ taki, że γ dopełnia β do α, to taki typ jest dokładnie jeden. Mianowicie, jeśli β jest typem odcinka $[x, z]$ takiego, że $n_{x,z} = i$, to γ jest typem odcinka, dla którego $n_{z,y} = n-i$ (gdzie $n_{x,y} = n$). Oznaczając $\left\langle {n \atop i} \right\rangle = \left\langle {\alpha \atop \beta, \gamma} \right\rangle$ $(n = n_{x,y}$, gdzie $\alpha = \overline{[x, y]}$, $i = n_{x,z}$, gdzie $\beta = \overline{[x, z]})$, stwierdzamy najpierw, że definicja $\left\langle {n \atop i} \right\rangle$ jest poprawna (bowiem typ wyznaczony jest przez

długość łańcucha maksymalnego). Typy nasze numerowane są liczbami naturalnymi (z zerem). Zatem z twierdzenia 2.2 otrzymujemy:

$$(2.1)\qquad f*g(n)=\sum_{i=0}^{n}\left\langle {n \atop i}\right\rangle f(i)\,g(n-i),$$

gdzie

$$(2.2)\qquad \left\langle {n \atop i}\right\rangle=\frac{b_n}{b_i\cdot b_{n-1}}.$$

TWIERDZENIE 2.3. *Jeśli* $\boldsymbol{P}=\langle P,\leqslant\rangle$ *ma własność dwumianową, to odwzorowanie* Φ *określone wzorem*

$$\Phi(f)=\sum_{n=0}^{\infty}\frac{f(n)}{b_n}x^n$$

jest izomorfizmem pomiędzy $\mathscr{R}(\boldsymbol{P})$ *oraz algebrą szeregów formalnych* $\boldsymbol{C}[\![x]\!]$.

Dowód. Oczywiście odwzorowanie Φ jest różnowartościowe, „na" i zachowuje 0. Φ zachowuje też jedynkę, łatwo bowiem zauważyć, że δ (jako funkcja na zbiorze N_0) ma postać: $\delta(0)=1$, $\delta(n)=0$ dla $n>0$. Zachowana jest też oczywiście suma i mnożenie przez liczbę. Dla pełności dowodu należy zatem wykazać, że Φ zachowuje mnożenie, tzn. że

$$\Phi(f*g)=\Phi(f)\cdot\Phi(g),$$

gdzie symbol po prawej stronie równości oznacza iloczyn szeregów formalnych. Mamy

$$\Phi(f)\,\Phi(g)=\left(\sum_{n=0}^{\infty}\frac{f(n)}{b_n}x^n\right)\left(\sum_{n=0}^{\infty}\frac{g(n)}{b_n}x^n\right)=\sum_{n=0}^{\infty}\left(\sum_{j=0}^{n}\frac{f(j)}{b_j}\cdot\frac{g(n-j)}{b_{n-j}}\right)x^n=$$
$$=\sum_{n=0}^{\infty}\left(\frac{1}{b_n}\sum_{j=0}^{n}\frac{b_n}{b_j\,b_{n-j}}f(j)\,g(n-j)\right)x^n.$$

Porównując prawą stronę ostatniej równości ze wzorami (2.1) i (2.2) otrzymujemy

$$\sum_{n=0}^{\infty}\frac{1}{b_n}\left(\sum_{j=0}^{n}\left\langle {n \atop j}\right\rangle f(j)\,g(n-j)\right)x^n=\sum_{n=0}^{\infty}\frac{f*g(n)}{b_n}x^n,$$

co kończy dowód. □

Zbadamy teraz kilka przykładów zbiorów $\langle P,\leqslant\rangle$ z własnością dwumianową oraz odpowiadające izomorfizmy z algebrą szeregów formalnych.

1. $\boldsymbol{P}_1=\langle N_0,\leqslant\rangle$. W tym przypadku $n_{x,y}$ to po prostu $y-x$ (jeśli $y\geqslant x$) oraz 0 (jeśli $y<x$). Liczba b_n jest zawsze równa 1, zatem $\left\langle {n \atop i}\right\rangle=1$. W ten sposób

stwierdzamy, że $\mathscr{R}(P_1)$ jest izomorficzna z algebrą szeregów formalnych poprzez izomorfizm Φ:

$$\Phi(f) = \sum_{n=0}^{\infty} f(n) x^n.$$

Szeregi formalne tej postaci, tj. $\sum_{n=0}^{\infty} a_n x^n$ nazywamy *funkcjami tworzącymi zwyczajnymi*. Zauważmy, że

$$\Phi(\zeta) = \sum_{n=0}^{\infty} x^n = (1-x)^{-1}, \qquad \Phi(\mu) = 1-x.$$

2. $P_2 = \langle \mathscr{P}_{\text{fin}}(N_0), \subseteq \rangle$. Dla zbioru P_2, $n_{x,y}$ to liczność różnicy $y-x$, jeśli $x \leqslant y$, lub 0 w przeciwnym przypadku. Liczba b_n wynosi $n!$. Istotnie, niech $|y-x| = n$, $y-x = \{a_1, \ldots, a_n\}$. Wtedy każda permutacja π liczb $1, \ldots, n$ wyznacza następujący łańcuch maksymalny pomiędzy x i y:

$$x,\ x \cup \{a_{\pi(1)}\},\ x \cup \{a_{\pi(1)}, a_{\pi(2)}\}, \ldots, x \cup \{a_{\pi(1)}, a_{\pi(2)}, \ldots, a_{\pi(n)}\} = y.$$

Odwrotnie, każdy łańcuch maksymalny musi mieć długość n (tj. liczy $n+1$ elementów) i wyznacza odpowiednią permutację. Izomorfizm algebry $\mathscr{R}(P_2)$ z $C[[x]]$ wyznacza nam odwzorowanie

$$\Phi(f) = \sum_{n=0}^{\infty} f(n) \frac{x^n}{n!},$$

szeregi formalne zaś tej postaci, tj. $\sum_{n=0}^{\infty} a_n \frac{x^n}{n!}$, nazywamy *funkcjami tworzącymi eksponencjalnymi*. Mamy

$$\Phi(\zeta) = e^x, \qquad \Phi(\mu) = e^{-x}.$$

Zauważmy, że w tym przypadku $\left\langle {n \atop i} \right\rangle = \frac{n!}{i!(n-i)!} = \binom{n}{i}$, co tłumaczy przyjęty przez nas symbol i wskazuje czego uogólnieniem jest $\left\langle {n \atop i} \right\rangle$.

3. $P_3 = \langle S, \subseteq \rangle$, gdzie S jest rodziną wszystkich skończenie wymiarowych podprzestrzeni pewnej nieskończenie wymiarowej przestrzeni liniowej nad ciałem skończonym $GF(q)$. W tym przypadku $n_{U,V} = \dim V - \dim U$ dla $U \subseteq V$. Obliczmy teraz b_n. Niech $\dim U = k$, $\dim V = k+n$, $U \subseteq V$. Dla każdego spośród $q^{k+n} - q^k$ elementów $e \in V \setminus U$ zbiór $U \cup \{e\}$ generuje pewną $(k+1)$-wymiarową podprzestrzeń U', $U \subseteq U' \subseteq V$, przy czym każda taka podprzestrzeń U jest generowana przez $q^{k+1} - q^k$ różnych elementów $e \in U' \setminus U$. Stąd liczba bezpośrednich następników elementu U w odcinku $[U, V]$ jest równa

$$\frac{q^{k+n} - q^k}{q^{k+1} - q^k} = \frac{q^n - 1}{q - 1} = \sum_{i=0}^{n-1} q^i.$$

Powtarzając to rozumowanie otrzymujemy

$$b_n = \prod_{j=0}^{n-1} \sum_{i=0}^{j} q^i.$$

Liczba ta jest oczywiście zależna jedynie od n, jako że każde dwa odcinki $[U, V]$, $[U', V']$, gdzie $U \subseteq V$, $U' \subseteq V'$, $\dim V - \dim U = \dim V' - \dim U' = n$, są izomorficzne z kratą podprzestrzeni n-wymiarowej przestrzeni ilorazowej V/U. Izomorfizm algebry $\mathcal{R}(\boldsymbol{P}_3)$ z $\boldsymbol{C}[\![x]\!]$ jest więc wyznaczony przez

$$\Phi(f) = \sum_{n=0}^{\infty} f(n) \frac{x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})}.$$

Szeregi formalne powyższej postaci nazywamy *funkcjami tworzącymi Eulera*. Mamy

$$\Phi(\zeta) = \sum_{n=0}^{\infty} \frac{x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})},$$

oraz uwzględniając wzór na funkcję Möbiusa kraty $\mathcal{L}(n, q)$ (por. rozdz. 2, twierdzenie 3.11):

$$\Phi(\mu) = \left(\sum_{n=0}^{\infty} \frac{x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})}\right)^{-1} =$$

$$= \sum_{n=0}^{\infty} (-1)^n q^{\binom{n}{2}} \frac{x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})}.$$

Mamy też oczywiście $\left\langle {n \atop i} \right\rangle = \binom{n}{i}_q$, gdzie $\binom{n}{i}_q$ jest współczynnikiem Gaussa (por. rozdz. 1 § 12,).

Uwaga. Funkcje tworzące Eulera definiuje się często nieco inaczej, jako

$$\sum_{n=0}^{\infty} f(n) \frac{x^n}{(1-q)(1-q^2)\dots(1-q^n)}.$$

Modyfikacja ta odpowiada zamianie zmiennej x na $x/(1-q)$.

4. $\boldsymbol{P}_4 = \langle T, \subseteq \rangle$, gdzie T składa się z „prostokątów” $R \times S$, gdzie $R \underset{\text{fin}}{\subseteq} \boldsymbol{N}_0$, $S \underset{\text{fin}}{\subseteq} \boldsymbol{N}_0$, $|R| = |S|$.

Stosując rozumowanie z punktu 2 stwierdzamy, że $b_n = (n!)^2$, $\left\langle {n \atop i} \right\rangle = \binom{n}{i}^2$, $n_{\langle R_1, S_1 \rangle, \langle R_2, S_2 \rangle} = |R_2 - R_1|$ (jeśli $R_1 \subseteq R_2$ i $S_1 \subseteq S_2$), zaś

$$\Phi(f) = \sum_{n=0}^{\infty} f(n) \frac{x^n}{(n!)^2}.$$

5. Zbiór $\boldsymbol{P}_5 = \langle \boldsymbol{N}, | \rangle$ nie ma własności dwumianowej. Łatwo zauważyć, że jeśli $x|y$, $x = p_1^{\alpha_1}, \dots, p_n^{\alpha_n}$, $y = p_1^{\beta_1} \dots p_n^{\beta_n}$, to każdy łańcuch maksymalny pomiędzy x i y

ma długość $|\beta_1-\alpha_1|+\ldots+|\beta_n-\alpha_n|$. Spełniona jest więc pierwsza część definicji własności dwumianowej. Jednakże druga część nie zachodzi: na przykład każdy łańcuch pomiędzy 1 i 2^5 ma długość 5, tak samo jak dla 1 i $3\cdot 2^4$. Jednakże odcinki $[1, 2^5]$ i $[1, 3\cdot 2^4]$ nie są izomorficzne; w szczególności mają różną liczbę łańcuchów maksymalnych.

Konstrukcję zredukowanej algebry incydencji możemy jednak zmodyfikować w przypadku zbioru $\boldsymbol{P}_5$ w następujący sposób. Określmy na zbiorze niepustych odcinków zbioru $\langle \boldsymbol{N}, |\rangle$ relację równoważności $\approx$ tak, by

$$[m, n] \approx [k, l] \Leftrightarrow \frac{n}{m} = \frac{l}{k}.$$

Łatwo zauważyć, że relacja ta indukuje na zbiorze niepustych odcinków podział *drobniejszy* niż podział na klasy izomorfizmu. W podobny sposób jak poprzednio można się przekonać, że funkcje stałe na klasach relacji $\approx$ tworzą podalgebrę – oznaczmy ją przez $\mathcal{R}(\boldsymbol{P}_5, \approx)$ – algebry $\mathcal{A}(\boldsymbol{P}_5)$. Jeśli typ odcinka $[k, l]$, tzn. klasę abstrakcji relacji $\approx$ zawierającą ten odcinek, identyfikujemy z liczbą l/k, a funkcje z $\mathcal{R}(\boldsymbol{P}_5, \approx)$ traktujemy jako określone na typach względem relacji $\approx$, to splot w $\mathcal{R}(\boldsymbol{P}_5, \approx)$ wyraża się wzorem

$$f*g(n) = \sum_{k,l} \left\langle {n \atop k,l} \right\rangle f(k)g(l),$$

gdzie

$$\left\langle {n \atop k, l} \right\rangle = \begin{cases} 1, & \text{jeśli } n = kl, \\ 0, & \text{w przeciwnym przypadku} \end{cases}$$

– podobnie jak w przypadku $\mathcal{R}(\boldsymbol{P})$, gdy $\boldsymbol{P}$ ma własność dwumianową (por. twierdzenie 2.2). Innymi słowy

$$f*g(n) = \sum_{i:\,i|n} f(i)g(n/i),$$

i w konsekwencji odwzorowanie

$$\Phi(f) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$$

określa izomorfizm algebry $\mathcal{R}(\boldsymbol{P}_5, \approx)$ ze wspomnianą w § 1 algebrą szeregów formalnych Dirichleta (por. (1.1)). Warto zauważyć, że przy tym izomorfizmie funkcja ζ przechodzi na szereg $\Phi(\zeta) = \sum_{n=1}^{\infty} n^{-s}$, który definiuje funkcję zmiennej zespolonej s – ważną w teorii liczb – zwaną funkcją ζ Riemanna. Podobnie jak w przypadku funkcji Möbiusa μ w dowolnej algebrze incydencji, również funkcja ζ nawiązuje więc do pewnych klasycznych obiektów znanych z teorii liczb.

Na zakończenie tego paragrafu zauważmy jeszcze następującą prostą interpretację funkcji ζ^2:

$$\zeta^2(x, y) = \sum_{z \in [x,y]} \zeta(x, z)\zeta(z, y) = |[x, y]|$$

(por. rozdz. 2, zad. 6a). Równość ta w przypadku zbiorów $\boldsymbol{P}_1$, $\boldsymbol{P}_2$, $\boldsymbol{P}_3$ prowadzi do następujących tożsamości:

$$\left(\sum_{n=0}^{\infty} x^n\right)^2 = \sum_{n=0}^{\infty} (n+1)x^n,$$

$$\left(\sum_{n=0}^{\infty} \frac{x^n}{n!}\right)^2 = \sum_{n=0}^{\infty} 2^n \frac{x^n}{n!},$$

$$= \left(\sum_{n=0}^{\infty} \frac{x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})}\right)^2 =$$

$$= \sum_{n=0}^{\infty} \frac{G_{n,q}\, x^n}{(1+q)(1+q+q^2)\dots(1+q+\dots+q^{n-1})},$$

gdzie $G_{n,q}$ są liczbami Galois (p. rozdz. 1, (12.2)). Odpowiadają one równościom

$$|[x, y]| = n+1 \quad \text{dla } \langle \boldsymbol{N}_0, \leqslant \rangle,$$

$$|[x, y]| = 2^n \quad \text{dla } \langle \mathscr{P}_{\text{fin}}(\boldsymbol{N}_0), \subseteq \rangle,$$

$$|[x, y]| = G_{n,q} \quad \text{dla } \langle S, \subseteq \rangle$$

dla x, y takich, że długość maksymalnego łańcucha z x do y wynosi n.

§ 3. Tożsamości wielomianowe, zastosowania teorii operatorów liniowych (metoda Mullina i Roty [1])

W paragrafie tym przedstawimy teorię tłumaczącą zachodzenie pewnych klasycznych tożsamości wielomianowych. Tożsamości te związane są przede wszystkim z problematyką zliczania rozmaitych obiektów kombinatorycznych, a także z innymi zagadnieniami, np. z prawdopodobieństwem geometrycznym.

Zaczniemy od następującej definicji: *Ciągiem wielomianów typu dwumianowego* nazywamy każdy ciąg $\langle W_n(x)\rangle_{n=0}^{\infty}$ wielomianów o współczynnikach w ciele $\boldsymbol{C}$ spełniający następujące warunki:

(i) $\deg W_n(x) = n$,

(ii) $W_n(x+y) = \sum_{j=0}^{n} \binom{n}{j} W_j(x)\, W_{n-j}(y)$.

Najprostszym przykładem takiego ciągu jest oczywiście ciąg $W_n(x) = x^n$, a warunek (ii) w tym przypadku to nic innego jak wzór Newtona. Jednakże nie jest to przykład jedyny. Literatura matematyczna zawiera wiele innych przykładów.

STWIERDZENIE 3.1. *Następujące ciągi wielomianów są typu dwumianowego:*
(a) *silnia górna*

$$[x]^n = x(x+1)\dots(x+(n-1)),$$

(b) *silnia dolna*

$$[x]_n = x(x-1)\dots(x-(n-1)),$$

(c) *wielomiany Abela*

$$A_n(x) = x(x-na)^{n-1} \quad (a \text{ jest ustaloną liczbą zespoloną}),$$

(d) *wielomiany Laguerre'a*

$$L_n(x) = \sum_{k=1}^{n} (-1)^k \frac{n!}{k!} \binom{n-1}{k-1} x^k.$$

Tożsamości odpowiadające punktowi (ii) definicji ciągu dwumianowego dla wspomnianych wyżej ciągów nazywają się w literaturze odpowiednio *wzorami Nörlunda, Vandermonde'a, Abela i Laguerre'a* — od nazwisk ich odkrywców.

Dowody tych — i innych pokrewnych — tożsamości zostały uzyskane metodami analitycznymi (por. też rozdz. 1 zad. 44). Rozwinięta w tym paragrafie teoria dostarczy jednolitej metody dowodu wszystkich tych tożsamości.

Zauważmy najpierw — nim przejdziemy do właściwej teorii — że na mocy punktu (i) definicji każdy ciąg dwumianowy jest bazą w przestrzeni liniowej wielomianów (nad ciałem C). Dalej zauważmy, że jeśli $\langle W_n(x)\rangle_{n=0}^{\infty}$, $\langle V_n(x)\rangle_{n=0}^{\infty}$ są ciągami typu dwumianowego, to w rozwinięciu $W_n(x)$ względem ciągu $\langle V_n(x)\rangle_{n=0}^{\infty}$ występują ze współczynnikami niezerowymi co najwyżej wyrazy $V_0(x), \dots, V_n(x)$.

Bezpośrednio z warunku (ii) wynika, że jeśli $\langle W_n(x)\rangle_{n=0}^{\infty}$ jest ciągiem typu dwumianowego, to $W_0(x) = 1$, gdyż $W_0(x)$ jest wielomianem stałym. Wielomiany $W_n(x)$ dla $n > 0$ mają wyraz wolny równy zeru, czyli $W_n(0) = 0$ dla $n > 0$. Faktu tego dowodzimy przez indukcję. Dla $n = 1$ mamy, wobec $W_0(x) \equiv 1$ i własności (i),

$$W_1(x+y) = W_1(x) + W_1(y).$$

Przyjmując $y = 0$ otrzymujemy $W_1(x) = W_1(x) + W_1(0)$, a więc $W_1(0) = 0$. Dalszy dowód indukcyjny jest nader prosty i pozostawiamy go Czytelnikowi.

Dalsze własności ciągów typu dwumianowego poznamy poniżej. Czytelnik może też znaleźć szczegółową analizę własności ciągów typu dwumianowego jak i alternatywną charakteryzację takich ciągów w pracy Kreida [1]; por. zadania 14 i 15.

Zajmiemy się teraz operatorami liniowymi, to znaczy przekształceniami liniowymi przestrzeni liniowej wielomianów. Tak więc każdy operator liniowy Q spełnia warunek:

$$Q[aW(x)+bV(x)] = aQ(W(x)) + bQ(V(x)), \qquad a, b \in C.$$

Jest rzeczą oczywistą, że operator liniowy wystarczy określić na elementach (dowolnej) bazy naszej przestrzeni. Na mocy liniowości rozszerza się on wtedy jednoznacznie na całą przestrzeń. Będziemy korzystali z tej konwencji podając poniższe przykłady. W dalszych naszych rozważaniach będą odgrywały rolę następujące operatory:

operator identycznościowy:

$$Ix^n = x^n,$$

operator przesunięcia o a:

$$E^a x^n = (x+a)^n,$$

(a jest tu parametrem, zadaną liczbą zespoloną lub wielomianem),

operator różniczkowania:

$$Dx^n = nx^{n-1},$$

operator wartości w punkcie a:

$$K^a x^n = a^n, \qquad a \in \mathbf{C},$$

operator mnożenia przez x:

$$M^x x^n = x^{n+1}.$$

Operatory można oczywiście składać; działanie to nie jest na ogół przemienne. Zachodzi jednak dla dowolnego a równość:

$$DE^a = E^a D. \tag{3.1}$$

Innymi słowy operator różniczkowania jest przemienny z przesunięciami, albo, jak będziemy mówili poniżej, niezmienniczy ze względu na przesunięcia.

Będziemy używali notacji D^k dla oznaczenia k-krotnego złożenia operatora różniczkowania. Jest to oczywiście operator liniowy, a z równości (3.1) wynika natychmiast przez indukcję

$$D^k E^a = E^a D^k.$$

Operatory nasze działają na wielomianach, dla każdego wielomianu $W(x)$ istnieje więc liczba k taka, że dla $m \geqslant k$ mamy $D^m W(x) = 0$. Taką liczbą k jest oczywiście $\deg(W(x))+1$. To z kolei pozwala nam rozpatrywać szeregi formalne operatorów postaci $\sum\limits_{k=0}^{\infty} a_k D^k$ (przyjmując $D^0 = I$). Mianowicie operator ten działa na wielomian stopnia n tak jak $\sum\limits_{k=0}^{n} a_k D^k$. Przy tym współczynniki a_k mogą same być operatorami liniowymi (mnożenie ma tu zatem sens złożenia; w szczególnym przypadku, gdy a_k jest liczbą, mamy tu do czynienia ze złożeniem z operatorem

liniowym mnożenia przez stałą). Przyjmijmy $K = K^0$, to znaczy branie wartości w punkcie 0. Mamy wtedy:

$$I = \sum_{k=0}^{\infty} \frac{x^k}{k!} KD^k, \qquad E^y = \sum_{k=0}^{\infty} \frac{y^k}{k!} D^k.$$

Czytelnik stwierdzi bez trudu prawdziwość powyższych wzorów sprawdzając wartości odpowiednich operatorów na elementach wybranej bazy, powiedzmy $\langle x^n \rangle_{n=0}^{\infty}$. Pierwszy z nich jest inną formą formuły Taylora (przypomnijmy, że mówi ona, iż $W(x) = \sum_{k=0}^{n} \frac{(D^k W)(0)}{k!} x^k$, gdzie $W(x)$ jest wielomianem stopnia n), a drugi jest jej uogólnieniem. Ze względu na formalne podobieństwo E^y oznaczamy czasem e^{yD}.

Mówimy, że operator liniowy Q jest *niezmienniczy ze względu na przesunięcia*, jeśli dla każdego y zachodzi:

$$E^y Q = QE^y.$$

Przypomnijmy, że operator różniczkowania i wszystkie jego iteracje są niezmiennicze ze względu na przesunięcia.

Delta operatorem nazywamy każdy operator liniowy Q, który jest niezmienniczy ze względu na przesunięcia i dla którego Qx jest stałą różną od zera.

Oczywiście operator różniczkowania D jest delta operatorem. Nazwa delta operatorów bierze się stąd, iż prototypem dla nich jest operator $E^1 - I$, powszechnie oznaczany przez Δ („delta"). Innych przykładów delta operatorów dostarczają operatory $\nabla = I - E^{-1}$, DE^a (*operator Abela*), $E^{1/2} - E^{-1/2}$ i $\frac{1}{2}(I + E^1)$ (*średnia Eulera*). Bardziej skomplikowane przykłady to używane w rachunku prawdopodobieństwa i statystyce operatory przekształcające wielomian $p(x)$ na $\int_x^{x+1} p(t)\,dt$ (*operator Bernoulliego*) lub na $\sqrt{2/\pi} \int_{-\infty}^{+\infty} e^{-t^2/2} p(x+t)\,dt$.

Delta operatory mają wiele własności analogicznych do operatora różniczkowania.

LEMAT 3.2. *Niech Q będzie delta operatorem. Wówczas*

(a) $Qa = 0$, *dla każdego wielomianu stałego a.*

(b) *Jeśli $W(x)$ jest wielomianem stopnia $n > 0$, to $QW(x)$ jest niezerowym wielomianem stopnia $n-1$.*

Dowód. (a) Skoro Q jest niezmienniczy ze względu na przesunięcia, zatem

$$QE^a x = E^a Qx.$$

Na mocy założenia istnieje c takie, że $Qx = c$. Mamy zatem $QE^a x = Q(x+a) = Qx + Qa = c + Qa$. Równocześnie $QE^a x = E^a Qx = E^a c = c$. Stąd $Qa = 0$.

(b) Wystarczy wykazać twierdzenie dla wielomianów $W(x) = x^n$, a następnie skorzystać z liniowości operatora Q. Dowodzimy tego przez indukcję względem n.

Dla $n = 1$ dowodzona własność jest częścią definicji. Zakładając prawdziwość tezy dla wszystkich k mniejszych albo równych n, dowodzimy teraz naszej tezy dla $n+1$. Mamy

$$QE^a x^{n+1} = Q(x+a)^{n+1} = Q\sum_{k=0}^{n+1}\binom{n+1}{k}a^k x^{n+1-k} = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k Qx^{n+1-k}.$$

Przyjmując $Qx^{n+1} = r(x)$ otrzymujemy

$$QE^a x^{n+1} = E^a Qx^{n+1} = r(x+a).$$

Stąd

$$r(x+a) = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k Qx^{n+1-k}.$$

Dla x równego zero otrzymujemy następujący wielomian zmiennej a:

$$r(a) = \sum_{k=0}^{n+1}\binom{n+1}{k}a^k [Qx^{n+1-k}]_{x=0}.$$

Wynika stąd, iż r jest wielomianem stopnia co najwyżej $n+1$. Wykażemy zatem, że współczynnik a^{n+1} jest w $r(a)$ równy 0, zaś odpowiedni współczynnik przy a^n jest różny od zera. Istotnie, współczynnik przy a^{n+1} jest równy

$$\binom{n+1}{n+1}[Qx^{n+1-(n+1)}]_{x=0} = \binom{n+1}{n+1}[Q1]_{x=0} = 0.$$

Natomiast współczynnik przy a^n jest równy

$$\binom{n+1}{n}[Qx]_{x=0} = (n+1)\cdot c \neq 0. \ \square$$

Wprowadzimy teraz pojęcie bazy dla delta operatora. Będziemy mówili, że ciąg $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest *bazą dla operatora* Q, jeśli każdy z wielomianów $w_n(x)$ jest stopnia n oraz

(i) $w_0(x) = 1$,
(ii) $w_n(0) = 0$ dla $n > 0$,
(iii) $Qw_n(x) = nw_{n-1}(x)$.

Oczywiście ciąg wielomianów $\langle x^n\rangle_{n=0}^{\infty}$ jest bazą dla operatora D, i to bazą jedyną, co wynika z następującego twierdzenia:

TWIERDZENIE 3.3. *Każdy delta operator ma dokładnie jedną bazę.*

Dowód. Skonstruujemy żądaną jedyną bazę $\langle w_n(x)\rangle_{n=0}^{\infty}$ delta operatora Q przez indukcję. Wiemy, że $w_0(x) = 1$. Załóżmy, że $n > 0$ i że znamy już wielomian $w_{n-1}(x)$. Z lematu 3.2 (b) wynika, że ciąg $\langle Qx^k\rangle_{k=1}^{\infty}$ jest bazą przestrzeni

wielomianów, ponieważ jego n-ty wyraz ma stopień $n-1$. Zatem równanie

$$\sum_{i=1}^{n} a_i Qx^i = nw_{n-1}(x)$$

ma dokładnie jedno rozwiązanie $a_1, \ldots, a_n$. Wobec tego wielomian $w_n(x) = \sum_{i=1}^{n} a_i x^i$ jest jedynym wielomianem stopnia n takim, że $w_n(0) = 0$ i $Qw_n(x) = nw_{n-1}(x)$. □

Przedstawimy teraz główny wynik tego paragrafu:

TWIERDZENIE 3.4 (Mullin, Rota [1]). *Na to, by ciąg* $\langle w_n(x)\rangle_{n=0}^{\infty}$ *był bazą dla pewnego delta operatora, potrzeba i wystarcza, by był on typu dwumianowego.*

Dowód. Niech $\langle w_n(x)\rangle_{n=0}$ będzie bazą dla delta operatora Q. Iterując równość (iii) otrzymujemy

$$Q^k w_n(x) = n(n-1)\ldots(n-(k-1))w_{n-k}(x) = [n]_k w_{n-k}(x).$$

Dla $k = n$ mamy zatem $Q^n w_n(x) = n!$.

Innymi słowy $[Q^n w_n(x)]_{x=0} = n!$, zaś $[Q^k w_n(x)]_{x=0} = 0$ dla $k < n$. Dla $k > n$ $Q^k w_n(x) = 0$, a zatem

$$w_n(x) = \sum_{k=0}^{\infty} \frac{w_k(x)}{k!} [Q^k w_n(x)]_{x=0}.$$

Jednakże każdy wielomian jest kombinacją liniową wielomianów z ciągu $\langle w_n(x)\rangle_{n=0}^{\infty}$ i wobec tego, korzystając ze skończoności rozwinięcia stwierdzamy, że dla dowolnego wielomianu $W(x)$

$$W(x) = \sum_{k=0}^{\infty} \frac{w_k(x)}{k!} [Q^k W(x)]_{x=0}.$$

Przyjmując $W(x)$ równe $w_n(x+y)$ mamy

$$w_n(x+y) = \sum_{k=0}^{\infty} \frac{w_k(x)}{k!} [Q^k w_n(x+y)]_{x=0}. \tag{3.2}$$

Zbadajmy zatem czym są „współczynniki” $[Q^k w_n(x+y)]_{x=0}$. Zauważmy, że $w_n(x+y) = E^y w_n(x)$. Skoro Q jest operatorem niezmienniczym ze względu na przesunięcia, to Q^k ma także tę własność (wykazujemy to przez indukcję względem k), czyli

$$Q^k E^y = E^y Q^k.$$

Stąd

$$Q^k w_n(x+y) = Q^k E^y w_n(x) = E^y Q^k w_n(x) = E^y [n]_k w_{n-k}(x) =$$
$$= [n]_k E^y w_{n-k}(x) = [n]_k w_{n-k}(x+y).$$

Wobec tego

$$[Q^k w_n(x+y)]_{x=0} = [[n]_k w_{n-k}(x+y)]_{x=0} = [n]_k w_{n-k}(y).$$

Jednakże $\binom{n}{k} = [n]_k/k!$, a dla $k > n$, $Q^k w_n(x+y) = 0$ (traktujemy tu y jako parametr). Otrzymujemy wobec tego

$$w_n(x+y) = \sum_{k=0}^{n} \binom{n}{k} w_k(x)\, w_{n-k}(y).$$

Załóżmy teraz, że $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest ciągiem wielomianów typu dwumianowego. Celem naszym jest znalezienie delta operatora Q takiego, że ciąg nasz jest jego bazą. Skoro wielomiany $w_n(x)$ tworzą bazę przestrzeni liniowej wielomianów, Q zaś ma być operatorem liniowym, wystarczy zatem określić Q na elementach naszego ciągu. To z kolei wymuszone jest przez warunek (iii) bazy delta operatora. Przyjmujemy zatem $Q(w_n(x)) = nw_{n-1}(x)$. Skoro ciąg $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest typu dwumianowego, to warunki (i) i (ii) dla bazy są spełnione. Także Qx jest stałą różną od zera. Pozostaje zatem do sprawdzenia, że Q jest operatorem niezmienniczym ze względu na przesunięcia.

Zastosujmy operator QE^a do wielomianu $w_n(x)$. Korzystając z dwumianowości ciągu $\langle w_n(x)\rangle_{n=0}^{\infty}$ otrzymujemy

$$QE^a w_n(x) = Qw_n(x+a) = Q \sum_{k=0}^{n} \binom{n}{k} w_k(x)\, w_{n-k}(a) =$$

$$= \sum_{k=1}^{n} \binom{n}{k} kw_{k-1}(x)\, w_{n-k}(a) = n \sum_{k=1}^{n} \binom{n-1}{k-1} w_{k-1}(x)\, w_{n-k}(a) =$$

$$= n \sum_{k=0}^{n-1} \binom{n-1}{k} w_k(x)\, w_{(n-1)-k}(a) = nw_{n-1}(x+a) = E^a Q w_n(x).$$

Ponieważ ciąg $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest bazą w przestrzeni wielomianów, oznacza to, że $QE^a = E^a Q$ dla dowolnego $a \in \mathbf{C}$. Kończy to dowód twierdzenia. □

Szukanie ciągów typu dwumianowego sprowadza się więc do znajdowania delta operatorów. Będziemy zatem szukali „postaci normalnej" dla delta operatorów. Metoda ta także pochodzi od Mullina i Roty.

TWIERDZENIE 3.5. *Niech Q będzie delta operatorem o bazie $\langle w_n(x)\rangle_{n=0}^{\infty}$. Operator liniowy S jest niezmienniczy ze względu na przesunięcia wtedy i tylko wtedy, gdy istnieje rozwinięcie*

$$S = \sum_{k=0}^{\infty} \frac{a_k}{k!} Q^k,$$

gdzie $a_k = [Sw_k(x)]_{x=0}$.

Dowód. Łatwo sprawdzić, że każdy operator postaci $\sum_{k=0}^{\infty} \frac{a_k}{k!} Q^k$ jest dobrze określonym operatorem liniowym i niezmienniczym ze względu na przesunięcia. Wykażemy teraz, iż operator S ma żądane rozwinięcie.

Korzystając z dwumianowości bazy $\langle w_n(x)\rangle_{n=0}^{\infty}$ operatora Q mamy, dla dowolnego $a \in \boldsymbol{C}$ i $n \in \boldsymbol{N}_0$,

$$w_n(x+a) = \sum_{k=0}^{n} \binom{n}{k} w_k(x) w_{n-k}(a) = \sum_{k=0}^{\infty} \frac{w_k(x)}{k!} (Q^k w_n)(a).$$

Zatem

$$Sw_n(x+a) = \sum_{k=0}^{\infty} \frac{Sw_k(x)}{k!} (Q^k w_n)(a)$$

i wobec tego

$$[SE^a w_n(x)]_{x=0} = \sum_{k=0}^{\infty} \frac{[Sw_k(x)]_{x=0}}{k!} (Q^k w_n)(a).$$

Korzystając z niezmienniczości operatora S wiemy, iż to wyrażenie jest równe

$$[E^a Sw_n(x)]_{x=0} = (Sw_n)(a).$$

Wynika stąd, że dla każdego $n \in \boldsymbol{N}_0$, wielomiany

$$Sw_n(x) \quad \text{oraz} \quad \sum_{k=0}^{\infty} \frac{[Sw_k(x)]_{x=0}}{k!} (Q^k w_n)(x)$$

także są sobie równe. Ponieważ ciąg $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest bazą przestrzeni wielomianów, wynika stąd równość operatorów liniowych

$$S = \sum_{k=0}^{\infty} \frac{[Sw_k(x)]_{x=0}}{k!} Q^k,$$

którą należało wykazać. □

Rozważmy dla przykładu operator $S = E^a$ (który jest oczywiście niezmienniczy ze względu na przesunięcia) i operator różniczkowania D. Bazą dla operatora D jest ciąg $\langle x^n\rangle_{n=0}^{\infty}$. Otrzymujemy zatem

$$E^a W(x) = \sum_{k=0}^{\infty} \frac{[E^a x^k]_{x=0}}{k!} (D^k W)(x),$$

czyli

$$W(x+a) = \sum_{k=0}^{\infty} \frac{a^k}{k!} (D^k W)(x);$$

po zamianie ról x i a otrzymujemy klasyczny wzór Taylora dla wielomianów (oczywiście suma po prawej stronie jest w istocie skończona).

Zauważmy teraz, że rodzina wszystkich operatorów liniowych tworzy algebrę z jedynką. Łatwo sprawdzić, że operatory niezmiennicze ze względu na przesunięcia tworzą podalgebrę tej algebry. Strukturę algebry operatorów niezmienniczych ze względu na przesunięcia charakteryzuje następujący rezultat:

Twierdzenie 3.6. *Niech Q będzie delta operatorem. Odwzorowanie Φ określone wzorem*

$$\Phi\left(\sum_{n=0}^{\infty} \frac{a_n}{n!} x^n\right) = \sum_{n=0}^{\infty} \frac{a_n}{n!} Q^n,$$

jest izomorfizmem algebry $\mathbf{C}[\![x]\!]$ i algebry operatorów niezmienniczych ze względu na przesunięcia.

Dowód. Z twierdzenia 3.5 wynika natychmiast, że tak określone odwzorowanie jest „na". Poprawność definicji, czyli to, że $\sum_{n=0}^{\infty} \frac{a_n}{n} Q^n$ jest operatorem liniowym, i to niezmienniczym ze względu na przesunięcia, jest oczywista. Jest też oczywiste, że odwzorowanie nasze zachowuje sumę. Sprawdzimy, że odwzorowanie to jest różnowartościowe i zachowuje iloczyn.

Jeśli

$$T = \sum_{n=0}^{\infty} \frac{a_n}{n!} Q^n = \sum_{n=0}^{\infty} \frac{n_n}{n!} Q^n,$$

to stosując operator T kolejno do wielomianów $w_n(x)$ z bazy operatora Q, stwierdzamy przez indukcję, iż $a_n = b_n$. To zaś oznacza różnowartościowość odwzorowania Φ.

Niech

$$T = \sum_{n=0}^{\infty} \frac{a_n}{n!} Q^n \quad \text{oraz} \quad S = \sum_{n=0}^{\infty} \frac{b_n}{n!} Q^n.$$

Aby wykazać, że $\Phi(TS) = \Phi(T)\Phi(S)$, wystarczy sprawdzić — zgodnie z twierdzeniem 3.5 — że

$$[(TS)\,w_n(x)]_{x=0} = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k}.$$

Mamy jednak

$$(TS)\,w_n(x) = \left(\sum_{k=0}^{\infty} \frac{a_k}{k!} Q^k\right)\left(\sum_{k=0}^{\infty} \frac{b_k}{k!} Q^k\right) w_n(x) = \sum_{k=0}^{\infty} \sum_{j=0}^{\infty} \frac{a_k b_j}{k!\,j!} Q^{k+j}(w_n(x)).$$

Jednakże $Q^{k+j} w_n(x) = [n]_{k+j} w_{n-(k+j)}(x)$, co oznacza, że $Q^{k+j} w_n(x) = 0$ dla $k+j > 0$. Zatem $[Q^{k+j} w_n(x)]_{x=0} = 0$ dla $k+j \neq n$, oraz $[Q^n w_n(x)]_{x=0} = n!$, gdyż

$w_0(x) = 1$. Wobec powyższego

$$[(TS)w_n(x)]_{x=0} = \sum_{k,j:\,k+j=n} \frac{n!}{k!\,j!} a_k b_j = \sum_{k=0}^{n} \binom{n}{k} a_k b_{n-k},$$

co kończy dowód. □

Wniosek 3.7. *W algebrze operatorów niezmienniczych ze względu na przesunięcia składanie jest działaniem przemiennym.* □

(Wniosek ten można też wyprowadzić bezpośrednio z twierdzenia 3.5).

Wniosek 3.8. *Operator Q jest niezmienniczy ze względu na przesunięcia wtedy i tylko wtedy, gdy istnieje ciąg $\langle a_n \rangle_{n=0}^{\infty}$ taki, że $Q = \sum_{n=0}^{\infty} a_n D^n$.* □

Z twierdzenia 3.6 wynika też natychmiast

Wniosek 3.9. *Niech Q będzie operatorem niezmienniczym ze względu na przesunięcia. Wówczas Q jest operatorem odwracalnym wtedy i tylko wtedy, gdy $Q1 \neq 0$.* □

Na koniec otrzymujemy poszukiwaną postać kanoniczną delta operatorów.

Twierdzenie 3.10. (Mullin i Rota [1]). *Operator Q jest delta operatorem wtedy i tylko wtedy, gdy istnieje ciąg $\langle a_n \rangle_{n=1}^{\infty}$ taki, że $a_1 \neq 0$ i $Q = \sum_{n=1}^{\infty} a_n D^n$.*

Dowód. Operator $Q = \sum_{n=1}^{\infty} a_n D^n$, gdzie $a_1 \neq 0$, jest delta operatorem, jest bowiem niezmienniczy ze względu na przesunięcia (por. wniosek 3.8), zaś $Qx = a_1 \neq 0$. Odwrotnie, jeśli Q jest delta operatorem, to jest w szczególności niezmienniczy ze względu na przesunięcia. Zatem istnieje ciąg $\langle a_n \rangle_{n=0}^{\infty}$ taki, że $Q = \sum_{n=0}^{\infty} a_n D^n$. Wykażemy, że $a_0 = 0$ i $a_1 \neq 0$. Istotnie, dla wielomianu x mamy $Qx = a_0 x + a_1$. Lecz Qx jest niezerową stałą, zatem $a_0 = 0$ i $a_1 \neq 0$, czego należało dowieść. □

Wnioskujemy stąd, że delta operatory nie są odwracalne.

Dla stwierdzenia, że ciąg wielomianów $\langle w_n(x) \rangle_{n=0}^{\infty}$ jest typu dwumianowego, wystarczy znaleźć delta operator, dla którego jest on bazą. Korzystając z tej uwagi wykażemy stwierdzenie 3.1, którego dowód zapowiadaliśmy we wstępie do tego paragrafu.

(a) Dla silni górnej delta operatorem generującym nasz ciąg wielomianów jest operator $I - E^{-1}$. Znajdziemy jego rozwinięcie względem operatora różniczkowania D. Mamy, zgodnie z uwagami poprzedzającymi lemat 3.2,

$$E^{-1} = \sum_{j=0}^{\infty} \frac{(-1)^j}{j!} D^j,$$

a zatem

$$I-E^{-1}=\sum_{j=1}^{\infty}\frac{(-1)^{j+1}}{j!}D^j.$$

Istnienie tego rozwinięcia wskazuje, na mocy twierdzenia 3.10, że $I-E^{-1}$ jest delta operatorem.

Zbadajmy teraz działanie $I-E^{-1}$ na wielomianach postaci $[x]^n$. Mamy

$$(I-E^{-1})[x]^n=[x]^n-[x-1]^n=\big(x+(n-1)\big)[x]^{n-1}-(x-1)[x]^{n-1}=n[x]^{n-1}.$$

To zaś oznacza, że $\langle[x]^n\rangle_{n=0}^{\infty}$ jest bazą delta operatora $I-E^{-1}$, a więc ciągiem typu dwumianowego.

(b) Dla silni dolnej delta operatorem generującym jest $E-I$. Operator ten, na mocy rozumowania analogicznego do użytego w punkcie (a), ma rozwinięcie $\sum_{n=1}^{\infty}\frac{D^n}{n!}$, zatem na mocy twierdzenia 3.10, jest delta operatorem. Wreszcie $(E-I)[x]_n=[x+1]_n-[x]_n=n[x]_{n-1}$, co wykazujemy podobnie jak w (a).

(c) Dla wielomianów Abela $A_n(x)=x(x-na)^{n-1}$ delta operatorem generującym jest DE^a równy $\sum_{n=1}^{\infty}\frac{a^{n-1}}{(n-1)!}D^n$. Spełnianie warunków (i) i (ii) definicji bazy jest oczywiste. Ponadto

$$\begin{aligned}DE^aA_n(x)&=E^aDA_n(x)=E^aD\big(x(x-na)^{n-1}\big)=\\&=E^a\big((x-na)^{n-1}+x(n-1)(x-na)^{n-2}\big)=\\&=E^a\big(n(x-a)(x-na)^{n-2}\big)=n(x+a-a)(x+a-na)^{n-2}=\\&=nx\big(x-(n-1)a\big)^{n-2}=nA_{n-1}(x).\end{aligned}$$

(d) Dla wielomianów Laguerre'a $L_n(x)=\sum_{k=1}^{n}(-1)^k\frac{n!}{k!}\binom{n-1}{k-1}x^k$ delta operatorem generującym jest $D/(D-I)$.

Istotnie,

$$\frac{D}{D-I}=-D\sum_{k=0}^{\infty}D^k=-\sum_{k=0}^{\infty}D^{k+1}.$$

Zatem $D/(D-I)$ jest delta operatorem.

Nieco żmudne obliczenia potrzebne dla wykazania, iż

$$\big(D/(D-I)\big)L_n(x)=nL_{n-1}(x)$$

pozostawiamy Czytelnikowi, zauważając jedynie, iż

$$D/(D-I)=-D-D^2-D^3-\ldots-D^n-\ldots,$$

co pociąga za sobą równość

$$D/(D-I)\,L_n(x) = (-D-D^2-\ldots-D^n)\,L_n x = -\sum_{j=1}^{n} D^j L_n(x).$$

W powyższych przykładach, w miejsce „zgadywania" odpowiednich delta operatorów, można było użyć konstrukcji operatora dla danej bazy użytej w twierdzeniu 3.4. Po sprawdzeniu, że uzyskany operator jest delta operatorem wiemy, iż wyjściowy ciąg bazowy jest typu dwumianowego. Niemniej istotnym dla znajdowania tożsamości wielomianowych jest rozwiązanie problemu odwrotnego: mając dany delta operator znaleźć jego bazę. Po jej odnalezieniu twierdzenie 3.4 gwarantuje uzyskanie całej rodziny tożsamości. Pokażemy teraz jak można to zrobić.

TWIERDZENIE 3.11. *Jeżeli T jest operatorem niezmienniczym ze względu na przesunięcia, to operator $T' = TM^x - M^x T$ także ma tę własność. Ponadto, jeżeli $T = \sum_{k=0}^{\infty} \frac{a_k}{k!} D^k$, to $T' = \sum_{k=0}^{\infty} \frac{a_{k+1}}{k!} D^k$, czyli szereg dla T' jest formalną pochodną (względem D) szeregu dla T.*

Dowód. Sprawdzimy najpierw, że $E^a T' = T' E^a$, dla dowolnego $a \in \mathbf{C}$. Korzystając z definicji T' i niezmienniczości ze względu na przsunięcie operatora liniowego T znajdujemy.

$$E^a T' = E^a TM^x - E^a M^x T = TE^a M^x - M^{x+a} E^a T = TM^{x+a} E^a - M^{x+a} TE^a =$$
$$= (TM^x E^a - M^x TE^a) + (aTE^a - aTE^a) = T' E^a.$$

Zwróćmy teraz uwagę, że dla dowolnego $k \in N_0$ mamy

$$[T' x^k]_{x=0} = [Tx^{k+1} - xTx^k]_{x=0} = [Tx^{k+1}]_{x=0} = a_{k+1},$$

ponieważ ciąg $\langle x^n \rangle_{n=0}^{\infty}$ jest bazą operatora D. Oznacza to, że szereg dla T' jest formalną pochodną szeregu dla T. □

Operator $T' = TM^x - M^x T$ nazywamy *pochodną Pincherle'a* operatora T.

LEMAT 3.12. *Pochodna Pincherle'a ma następujące własności:*

(a)
$$I' = 0, \quad D' = I.$$

(b) *Dla dowolnych operatorów T i S mamy*

$$(TS)' = T'S + TS'.$$

(c) *Jeżeli T jest operatorem i $n \in N_0$, to*

$$(T^n)' = nT'T^{n-1}.$$

Jeżeli operator T jest odwracalny, to równość ta pozostaje w mocy dla dowolnej liczby całkowitej n.

Dowód. (a) Przez bezpośrednie sprawdzenie.

(b) Korzystając z definicji otrzymujemy

$$(TS)' = TSM^x - M^x TS = TM^x S - M^x TS + TSM^x - TM^x S =$$
$$= (TM^x - M^x T)S + T(SM^x - M^x S) = T'S + TS'.$$

(c) Przez indukcję, korzystając z (b). □

Zauważmy, że każdy delta operator Q daje się przedstawić w postaci $Q = DP$, gdzie P jest niezmienniczym ze względu na przesunięcia operatorem odwracalnym. W tym celu wystarczy rozwinąć Q, zgodnie z twierdzeniem 3.10, w szereg $Q = \sum_{n=1}^{\infty} a_n D^n$ i jako P przyjąć operator $\sum_{n=0}^{\infty} a_{n+1} D^n$. Wniosek 3.9 gwarantuje nam odwracalność operatora P.

Następujące twierdzenie pozwala nam na odnajdywanie bazy dla zadanego delta operatora.

Twierdzenie 3.13. (Mullin i Rota [1]). *Jeżeli ciąg wielomianów $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest bazą dla delta operatora $Q = DP$, to $w_0(x) = 1$, i dla każdego $n > 0$ mamy*

(a) $w_n(x) = Q' P^{-n-1} x^n$;

(b) $w_n(x) = P^{-n} x^n - (P^{-n})' x^{n-1}$;

(c) $w_n(x) = xP^{-n} x^{n-1}$;

(d) $w_n(x) = x(Q')^{-1} w_{n-1}(x)$.

W zależności od postaci konkretnych operatorów Q i P można użyć, dla obliczenia bazy, dowolnej z powyższych zależności. Jeszcze inna indukcyjna technika szukania bazy została wykorzystana w dowodzie twierdzenia 3.3.

Dowód. Oczywiście $w_0(x)$ musi być wielomianem stałym równym 1. Niech teraz $n \in N$. Zaczniemy od wykazania, że prawe strony równości (a), (b) i (c) określają ten sam ciąg wielomianów.

Korzystając z własności pochodnej Pincherle'a oraz przemienności składania operatorów niezmienniczych ze względu na przesunięcia — wniosek 3.7 — otrzymujemy

$$Q' P^{-n-1} = (DP)' P^{-n-1} = (D'P + DP') P^{-n-1} = P^{-n} + P' P^{-n-1} D =$$
$$= P^{-n} - (1/n)(P^{-n})' D.$$

Zatem, dla $n > 0$,

$$Q' P^{-n-1} x^n = P^{-n} x^n - (P^{-n})' x^{n-1} =$$
$$= P^{-n} x^n - (P^{-n} M^x - M^x P^{-n}) x^{n-1} = xP^{-n} x^{n-1}.$$

Wobec powyższego oznaczmy przez $v_n(x)$ wielomian $Q' P^{-n-1} x^n = P^{-n} x^n - (P^{-n})' x^{n-1} = xP^{-n} x^{n-1}$ dla $n > 0$, oraz wielomian stały 1 dla $n = 0$. Zatem, dla $n > 1$, $Qv_n(x) = DP(Q' P^{-n-1} x^n) = Q' P^{-n} Dx^n = nQ' P^{-n} x^{n-1} = nv_n(x)$. Czytelnik łatwo też sprawdzi, że $Qv_1(x) = v_0(x) = 1$. Można w tym celu użyć równości

$Qv_1(x) = Q(xP^{-1}1)$ i skorzystać z rozwinięć Q i P^{-1} względem operatora D. Ponadto równość $v_n(x) = xP^{-n}x^{n-1}$ zapewnia, że $v_n(0) = 0$ dla $n > 0$. Oznacza to, że ciąg $\langle v_n(x)\rangle_{n=0}^{\infty}$ jest bazą operatora Q i na mocy jedności bazy otrzymujemy $v_n(x) = w_n(x)$ dla dowolnego $n \in N_0$.

Równość (d) otrzymujemy wstawiając w (c) w miejsce x^{n-1} wyrażenie $P^n(Q')^{-1}w_{n-1}(x)$, które jest równe x^{n-1} na mocy (a). □

Przedstawiona powyżej metoda jest przypadkiem szczególnym ogólnego schematu, który pozwala na znajdowanie związków pomiędzy ciągami bazowymi różnych delta operatorów i który pokrótce opiszemy.

Niech C będzie delta operatorem i niech ciąg $\langle v_n(x)\rangle_{n=0}^{\infty}$ będzie jego bazą. Przez B oznaczymy operator liniowy taki, że $Bv_n(x) = v_{n+1}(x)$. Dowodzimy, że jeżeli T jest operatorem niezmienniczym ze względu na przesunięcia, to operator $T^{(C)} = TB - BT$ jest też niezmienniczy. A także, że jeżeli $T = \sum_{k=0}^{\infty} \frac{a_k}{k!} C^k$, to $T^{(C)} = \sum_{k=0}^{\infty} \frac{a_{k+1}}{k!} C^k$ (formalna pochodna względem C).

Dowód przesuwalności dla $T^{(C)}$ jest rachunkowo znacznie bardziej kłopotliwy od podobnego dowodu dla $T' = T^{(D)}$. Polega na wykazaniu, że $E^a T^{(C)} v_n(x)$ i $T^{(C)} E^a v_n(x)$ są sobie równe dla dowolnych $a \in \mathbf{C}$ i $n \in N_0$. Dla znalezienia wartości odpowiednich operatorów korzystamy z rozwinięcia operatora T względem C oraz z dwumianowości ciągu $\langle v_n(x)\rangle_{n=0}^{\infty}$. Aby znaleźć rozwinięcie dla $T^{(C)}$, sprawdzamy, jak poprzednio, że $[T^{(C)} v_k(x)]_{x=0} = [Tv_{k+1}(x)]_{x=0}$. Wynika to stąd, że rozwijając wielomian $B(Tv_k(x))$ w bazie $\langle v_n(x)\rangle_{n=0}^{\infty}$ otrzymamy z niezerowymi współczynnikami jedynie wielomiany $v_n(x)$ o indeksach większych od zera, a więc takie, że $v_n(0) = 0$. Szczegóły rachunkowe pozostawiamy Czytelnikowi.

Powtarzając, w zasadzie, dowód lematu 3.12 możemy pokazać następujące własności pochodnej $T^{(C)}$.

LEMAT 3.14. *Dla operatora* $T^{(C)}$ *mamy*:

(a) $$I^{(C)} = 0, \qquad C^{(C)} = I;$$

(b) *dla dowolnych operatorów* T *i* S *mamy*

$$(TS)^{(C)} = T^{(C)} S + TS^{(C)};$$

(c) *jeśli* T *jest operatorem i* $n \in N_0$, *to*

$$(T^n)^{(C)} = nT^{(C)} T^{n-1}.$$

Równość ta pozostaje w mocy dla dowolnej liczby całkowitej n, *o ile* T *jest odwracalny.*

Czytelnik może teraz bez żadnych istotnych zmian zaadaptować dowód twierdzenia 3.13 aby uzyskać następujący wynik.

TWIERDZENIE 3.15. *Niech* Q *i* C *będą delta operatorami o bazach odpowiednio* $\langle w_n(x)\rangle_{n=0}^{\infty}$ *i* $\langle v_n(x)\rangle_{n=0}^{\infty}$, *niech* P *będzie operatorem odwracalnym takim, że* $Q = CP$

i niech operator B odwzorowuje $v_n(x)$ *na* $v_{n+1}(x)$ *dla dowolnego* $n \in N_0$. *Wówczas* $w_0(x) = v_0(x) = 1$ *i dla każdego* $n > 0$ *mamy*

(a) $w_n(x) = Q^{(C)} P^{-n-1} v_{n-1}(x)$;
(b) $w_n(x) = P^{-n} v_n(x) - (P^{-n})^{(C)} v_{n-1}(x)$;
(c) $w_n(x) = BP^{-n} v_{n-1}(x)$;
(d) $w_n(x) = B(Q^{(C)})^{-1} w_{n-1}(x)$. □

Powróćmy jeszcze raz do naszych przykładów.

Dla operatora $\Delta = E - I$ mamy $\Delta' = E$. Wobec tego, jeżeli jego bazę oznaczymy przez $\langle w_n(x) \rangle_{n=0}^{\infty}$, to twierdzenie 3.13 daje nam

$$w_n(x) = xE^{-1} w_{n-1}(x) = x(x-1) E^{-1} w_{n-1}(x-1).$$

Łatwo wykazać przez indukcję, że $w_n(x) = [x]_n$, $n \in N_0$. Podobnie dla operatora $I - E^{-1} = \nabla$, dla którego $\nabla' = E$, otrzymujemy jako bazę ciąg $\langle [x]^n \rangle_{n=0}$ ($[x]_0 = [xx]^0 = 1$).

Operator Abela ma postać $E^a D$. Dzięki twierdzeniu 3.13 wiemy, że jego baza składa się z wielomianów postaci $xE^{-an} x^{n-1} = x(x-an)^{n-1}$.

Znajdźmy jeszcze bazę operatora $E^{1/2} - E^{-1/2} = \Delta E^{-1/2}$. Oznaczmy przez R operator $\sum_{n=0}^{\infty} D^n/(n+1)!$. Jak było zauważone uprzednio, $\Delta = DR$. Wobec tego $E^{1/2} - E^{-1/2} = D(RE^{-1/2})$ i $[x]_n = xR^{-n} x^{n-1}$. Zatem, dla $n > 0$, n-ty wielomian bazy operatora $E^{1/2} - E^{-1/2}$ ma postać

$$x(E^{-1/2} R)^{-n} x^{n-1} = xE^{n/2} R^{-n} x^{n-1} = xE^{n/2} \frac{[x]_n}{x} =$$
$$= xE^{n/2} [x-1]_{n-1} = x[x+n/2-1]_{n-1}.$$

Oczywiście, każdy z tych ciągów daje nam odpowiednią tożsamość wielomianową.

Zajmijmy się teraz ponownie wielomianami Laguerre'a. Niech będzie dany operator L, który odwzorowuje wielomian $p(x)$ na wielomian

$$-\int_0^{\infty} e^{-t} \frac{dp(x+t)}{dx} dt.$$

Całkując przez części otrzymujemy równość $Lx^n = (n+1)^{-1} Lx^{n+1} - x^n$ i stąd, przez indukcję, $[Lx^n]_{x=0} = -n!$. Wobec tego, korzystając z twierdzenia 3.5, mamy $L = D/(D-I)$. Z twierdzenia 3.13 natychmiast wynika, że

$$L_n(x) = x(D-I)^n x^{n-1} = x \sum_{k=1}^{n} \binom{n}{k} (-1)^k D^{n-k} x^{n-1} =$$
$$= x \sum_{k=1}^{n} (-1)^k \binom{n}{k} [n-1]_{n-k} x^k = \sum_{k=1}^{n} (-1)^k \frac{n!}{k!} \frac{[n-1]_{n-k}}{(n-k)!} x^k =$$
$$= \sum_{k=1}^{n} \frac{n!}{k!} \binom{n-1}{k-1} (-x)^k.$$

A więc rzeczywiście $D/(D-I)$ jest operatorem generującym dla wielomianów Laguerre'a, tak jak było stwierdzone uprzednio.

Zwróćmy uwagę, że

$$\frac{L}{L-I} = \frac{D}{D-I}\Big/\left(\frac{D}{D-I}-I\right) = D.$$

Wobec tego twierdzenie 3.15 daje nam natychmiast

$$x^n = B(L-I)^n L_{n-1}(x).$$

Powtarzając w zasadzie wykonany powyżej rachunek otrzymujemy

$$x^n = \sum_{k=1}^{n} \frac{n!}{k!}\binom{n-1}{k-1}(-1)^k L_k(x).$$

Zauważmy, że mamy także relację

$$\nabla = E^{-1}\Delta = \Delta/(\Delta+I) = -\Delta/(-\Delta-I).$$

Ponieważ, jak łatwo sprawdzić, bazą dla operatora $-\Delta$ jest ciąg $\langle(-x)^k\rangle_{k=0}^{\infty}$, więc, licząc jak wyżej, mamy

$$[x]^n = \sum_{k=1}^{\infty} \frac{n!}{k!}\binom{n-1}{k-1}(-1)^k[-x]^k = \sum_{k=1}^{\infty} \frac{n!}{k!}\binom{n-1}{k-1}[x]_k.$$

W podobny sposób

$$[x]_n = \sum_{k=1}^{\infty} \frac{n!}{k!}\binom{n-1}{k-1}(-1)^{n-k}[x]^k.$$

Liczby $\frac{n!}{k!}\binom{n-1}{k-1}$ występujące w powyższych rozwinięciach są znane jako *liczby Laha* (por. rozdz. 2, zad. 12).

Uzyskanie dalszych tożsamości w podobnym stylu pozostawiamy Czytelnikowi. Szczególnie interesujące efekty można uzyskać rozwijając wielomian x^n w bazach $\langle[x]_k\rangle_{k=0}^{\infty}$ i $\langle[x]^k\rangle_{k=0}^{\infty}$, a także obliczając bazę operatora Bernoulliego.

§ 4. Notacja zaćmieniowa (umbralna), dalsze tożsamości wielomianowe

Wprowadzimy teraz technikę umożliwiającą otrzymanie wielu dalszych tożsamości wielomianowych. Użyjemy do tego — i uzasadnimy stosowanie — tzw. notacji umbralnej (zwanej też notacją Sylvestera). Przedtem jednak udowodnimy twierdzenie charakteryzujące operatory przeprowadzające pomiędzy sobą bazy delta operatorów. Przypomnijmy, że operatory niezmiennicze ze względu na przesunięcia tworzą podalgebrę algebry operatorów liniowych.

TWIERDZENIE 4.1 (Mullin i Rota [1]). *Niech P i Q będą delta operatorami o bazach odpowiednio $\langle w'_n(x)\rangle_{n=0}^{\infty}$ i $\langle w''_n(x)\rangle_{n=0}^{\infty}$. Niech T będzie operatorem liniowym takim, że dla każdego n, $Tw'_n(x) = w''_n(x)$. Wówczas:*

(a) *Operator T jest odwracalny;*

(b) *przekształcenie określone wzorem $S \mapsto TST^{-1}$ jest automorfizmem algebry operatorów niezmienniczych ze względu na przesunięcia, który przeprowadza delta operatory na delta operatory;*

(c) *jeśli $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest ciągiem typu dwumianowego, to ciąg $\langle Tw_n(x)\rangle_{n=0}^{\infty}$ jest także ciągiem typu dwumianowego.*

Dowód. (a) Określmy operator liniowy T^* przyjmując $T^* w''_n(x) = w'_n(x)$ dla każdego $n \in N_0$. Łatwo sprawdzić, że T^* jest operatorem odwrotnym do T.

(b) Dla wielomianów $w'_n(x)$ mamy równości

$$TP\,w'_n(x) = T\big(Pw'_n(x)\big) = Tnw'_{n-1}(x) =$$

$$= nTw'_{n-1}(x) = nw''_{n-1}(x) = Qw''_n(x) = QTw'_n(x).$$

Zatem, ze względu na liniowość operatorów TP i QT oraz fakt, że ciąg $\langle w'_n(x)\rangle_{n=0}^{\infty}$ jest bazą w przestrzeni $C[x]$, mamy

$$TP = QT.$$

Przez indukcję względem n wykazujemy teraz, że dla $n \in N$,

$$TP^n = Q^n T,$$

czyli $Q^n = TP^n T^{-1}$.

Niech teraz S będzie operatorem niezmienniczym ze względu na przesunięcia. Zgodnie z twierdzeniem 3.5 (o istnieniu rozwinięcia) istnieje ciąg $\langle a_n\rangle_{n=0}^{\infty}$ taki, że

$$S = \sum_{n=0}^{\infty} \frac{a_n}{n!} P^n.$$

Zatem

$$TST^{-1} = \sum_{n=0}^{\infty} \frac{a_n}{n!} TP^n T^{-1} = \sum_{n=0}^{\infty} \frac{a_n}{n} Q^n,$$

a ponieważ TST^{-1} ma rozwinięcie względem delta operatora Q, więc TST^{-1} jest elementem algebry operatorów niezmienniczych ze względu na przesunięcia.

Czytelnik bez trudu udowodni, że badane przekształcenie zachowuje działania na operatorach. Ponadto odwzorowanie $S \mapsto T^{-1}ST$ jest przekształceniem odwrotnym. Oznacza to, że nasze przekształcenie jest automorfizmem algebry operatorów niezmienniczych ze względu na przesunięcia.

Rozwijające dowolny delta operator do postaci $\sum_{n=0}^{\infty} \frac{a_n}{n!} P^n$ otrzymamy $a_0 = 0$

i $a_1 \neq 0$. Ponieważ jego obraz $\sum_{n=0}^{\infty} \frac{a_n}{n!} Q^n$ ma tę samą własność, jest on także delta operatorem. To kończy dowód punktu (b).

(c) Rozważmy delta operator R, którego bazą jest ciąg wielomianów $\langle w_n(x) \rangle_{n=0}^{\infty}$. Wykażemy, że ciąg $\langle Tw_n(x) \rangle_{n=0}^{\infty}$ jest bazą delta operatora $S = TRT^{-1}$. Mamy mianowicie

$$S(Tw_n(x)) = TRT^{-1}\, Tw_n(x) = Tnw_{n-1}(x) = n(Tw_{n-1}(x)).$$

Wystarczy zatem wykazać, że $Tw_n(0) = 0$ dla $n > 0$. Skoro $Tw_n'(x) = w_n''(x)$, to rozwinięcie $Tw_n(x)$ względem baz $\langle w_n''(x) \rangle_{n=0}^{\infty}$ ma te same współczynniki co rozwinięcie $w_n(x)$ względem bazy $\langle w_n'(x) \rangle_{n=0}^{\infty}$. Jednakże $w_n(0) = 0$ i współczynnik przy $w_0'(x)$ jest zerem. Wobec tego $Tw_n(0) = 0$. □

Możemy już teraz wprowadzić *notację umbralną*. Jeśli $\mathbf{w} = \langle w_n(x) \rangle_{n=0}^{\infty}$ jest ciągiem wielomianów, to operator liniowy $L_{\mathbf{w}}$ określamy – zadając go na bazie $\langle x^n \rangle_{n=0}^{\infty}$ – wzorem

$$L_{\mathbf{w}}(x^n) = w_n(x).$$

Operator $L_{\mathbf{w}}$ działa zatem na całej przestrzeni liniowej wielomianów $C[x]$ i obraz $L_{\mathbf{w}}(a_0 + \ldots + a_n x^n)$ jest równy $a_0 w_0(x) + \ldots + a_n w_n(x)$.

Wielomian $L_{\mathbf{w}}(V(x))$ oznaczamy symbolicznie $V(\mathbf{w})$. Na przykład dla wielomianu $V(x) = x$ mamy $\mathbf{w}(x) = w_1(x)$, $[\mathbf{w}(x)]^2 = w_2(x)$. W tej notacji $(\mathbf{w}(x) - a)(\mathbf{w}(x) + a) = w_2(x) - a^2 w_0(x)$, $(\mathbf{w}(x) + a)(\mathbf{w}(x) + a) = w_2(x) + 2aw_1(x) + a^2 w_0(x)$.

W ten sposób fakt, że ciąg $\langle w_n(x) \rangle_{n=0}^{\infty}$ jest typu dwumianowego zapisujemy symbolicznie

$$\mathbf{w}^n(x+y) = (\mathbf{w}(x) + \mathbf{w}(y))^n.$$

Jeśli $\langle w_n(x) \rangle_{n=0}^{\infty}$, $\langle v_n(x) \rangle_{n=0}^{\infty}$ są ciągami wielomianów, to ciąg $\langle u_n(x) \rangle_{n=0}^{\infty}$ określony wzorem

$$u_n(x) = w_n(\mathbf{v}(x)),$$

czyli

$$u_n = L_{\mathbf{v}}(w_n),$$

nazywamy *złożeniem umbralnym* ciągów $\mathbf{w}$ i $\mathbf{v}$. Zachodzi następujące twierdzenie.

TWIERDZENIE 4.2 (Rota, Kahaner i Odlyżko [1]). *Jeśli P i Q są delta operatorami o bazach odpowiednio $\mathbf{w} = \langle w_n(x) \rangle_{n=0}^{\infty}$, $\mathbf{v} = \langle v_n(x) \rangle_{n=0}^{\infty}$, przy czym $P = F(D)$, $Q = G(D)$ są odpowiednio rozwinięciami operatorów P i Q względem operatora pochodnej D* (por. tw. 3.10), *to złożenie umbralne ciągów $\mathbf{w}$ i $\mathbf{v}$ jest bazą dla delta operatora $F(G(D))$.*

Dowód. Zauważmy najpierw, że szereg G jest podstawialny do F, jego wyraz wolny jest bowiem zerem. Rozważmy $T = L_{\mathbf{v}}$. Na mocy twierdzenia 4.1 operator T

przeprowadza każdy ciąg typu dwumianowego na ciąg typu dwumianowego. Jeśli $w_n(x) = \sum_{j=0}^{n} a_j x^j$, to

$$Tw_n(x) = \sum_{j=0}^{n} a_j v_j = w_n(v(x)) = u_n(x).$$

Zatem ciąg $\langle u_n(x)\rangle_{n=0}^{\infty}$ jest typu dwumianowego i jest bazą dla operatora TPT^{-1}, którego rozwinięciem jest szereg $F(G(D))$, co łatwo sprawdzić. □

Niech $T = L_w$. Wówczas $T^{-1}(w_n(x)) = x^n$. Wobec twierdzenia 4.1, T^{-1} przeprowadza każdy ciąg typu dwumianowego na ciąg typu dwumianowego. Przyjmijmy $v_n(x) = T^{-1}x^n$. Wówczas $v(x) = \langle v_n(x)\rangle_{n=0}^{\infty}$ jest ciągiem typu dwumianowego oraz $Tv_n(x) = TT^{-1}x^n = x^n$. Jednakże $Tv_n(x) = w_n(v(x))$.

Z prostych rozważań algebraicznej natury wypływa następujący wniosek.

WNIOSEK 4.3. *Jeśli $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest ciągiem typu dwumianowego, to istnieje dokładnie jeden ciąg $v(x) = \langle v_n(x)\rangle_{n=0}^{\infty}$ taki, że*

$$w_n(v(x)) = x^n.$$

Co więcej wielomian $v_n(w(x))$ także równa się x^n. Każdy operator umbralny, czyli operator H taki, że $H(w_n(x)) = v_n(x)$, gdzie $w(x)$ i $v(x)$ są ciągami typu dwumianowego, jest postaci L_u dla pewnego ciągu typu dwumianowego, $u = \langle u_n(x)\rangle_{n=0}^{\infty}$. Mianowicie $u_n(x) = H(x^n)$. Fakt ten ma liczne zastosowania. Na przykład, jeśli $\langle w_n(x)\rangle_{n=0}^{\infty}$ jest bazą dla operatora $P = F(D)$, zaś $\langle v_n(x)\rangle_{n=0}^{\infty}$ jest bazą dla operatora $Q = G(D)$, to $G = H(F(t))$. Ta ostatnia równość pozwala znajdować delta operator R, którego bazą jest ciąg $\langle u_n(x)\rangle_{n=0}^{\infty}$. Na przykład, jeśli $w_n(x) = [x]^n$, $v_n(x) = x^n$, to $G(t) = t$, zaś $P(t) = 1-e^{-t}$. Zatem $H = -\ln(1-t)$, to znaczy $R = -\ln(I-D)$ (oczywiście mowa tu o „formalnym” logarytmie). Jeśli $v_n(x) = x^n$, zaś $w_n(x) = [x]_n$, to $G(t) = t$, $F(t) = e^t - 1$, zaś $H(t) = \ln(1+t)$. Wielomiany u_n otrzymane w tym przypadku, to tzw. wielomiany eksponencjalne (por. zad. 17).

Przykłady te oczywiście można mnożyć, lecz nie będziemy tu wnikali w te zagadnienia.

§ 5. Przykłady funkcji tworzących

Funkcje tworzące stanowią jedną z podstawowych technik kombinatoryki, musimy zatem nauczyć się operować ich aparatem. Izomorfizm algebry funkcji analitycznych z podalgebrą algebry szeregów formalnych pozwala nam przyjąć pewne „skróty” ułatwiające operowanie funkcjami tworzącymi (szeregami formalnymi).

Tożsamości i skróty, które teraz poznamy, są dwojakiego rodzaju. Pierwsze — to zależności pomiędzy funkcjami tworzącymi. Drugie — to system skrótów dla konkretnych funkcji tworzących. Tak więc rozpoczniemy od następującego

problemu. Znamy skrót dla szeregu $\sum_{n=0}^{\infty} a_n x^n$. Jaki jest skrót dla szeregu $\sum_{n=0}^{\infty} b_n x^n$, jeśli $\langle b_n \rangle_{n=0}^{\infty}$ zależy – w określony sposób – od $\langle a_n \rangle_{n=0}^{\infty}$. Drugi problem polega na szukaniu skrótów dla pewnych konkretnych ciągów współczynników szeregu.

Zaczniemy od zależności pomiędzy ciągami i odpowiednich równości dla funkcji tworzących. Umówmy się, że – jak uprzednio – symbol $\boldsymbol{a}$ oznacza ciąg $\langle a^n \rangle_{n=0}^{\infty}$, $f_{\boldsymbol{a}}(x)$ zaś jest szeregiem $\sum_{n=0}^{\infty} a_n x^n$.

TWIERDZENIE 5.1.

(a)
$$b_n = \begin{cases} 0, & n < k, \\ a_{n-k}, & n > k \end{cases}$$

jest równoważne równości

$$f_{\boldsymbol{b}}(x) = x^k f_{\boldsymbol{a}}(x).$$

(b) $b_n = a_{n+k}$ *jest równoważne równości*

$$f_{\boldsymbol{b}}(x) = \frac{1}{x^k}\left(f_{\boldsymbol{a}}(x) - (a_0 + a_1 x + \ldots + a_{k-1} x^{k-1})\right).$$

(c) $b_n = c^n a_n$ *jest równoważne równości*

$$f_{\boldsymbol{b}}(x) = f_{\boldsymbol{a}}(cx).$$

(d) $b_n = n a_n$ *jest równoważne równości*

$$f_{\boldsymbol{b}}(x) = x(Df_{\boldsymbol{a}})(x).$$

(e) $b_n = a_{n+1} - a_n$ *jest równoważne równości*

$$f_{\boldsymbol{b}}(x) = \frac{(1-x) f_{\boldsymbol{a}}(x) - f_{\boldsymbol{a}}(0)}{x}.$$

(f) $b_n = \sum_{j=0}^{n} a_j$ *jest równoważne równości*

$$f_{\boldsymbol{b}}(x) = \frac{f_{\boldsymbol{a}}(x)}{1-x}.$$

Dowód. Równoważności (a), (b) i (c) wynikają bezpośrednio z definicji; (d) wynika z (a) i z definicji pochodnej; (e) wynika z (b); (f) wynika z wielokrotnego stosowania (a) i pierwszego wzoru z następującej tabeli skrótów. □

Poniżej podano skróty dla niektórych konkretnych funkcji

$$a_n = 1, \qquad f_{\boldsymbol{a}} = \frac{1}{1-x},$$

$$a_n = n, \qquad f_{\boldsymbol{a}} = \frac{x}{(1-x)^2},$$

$$a_n = \binom{n+k-1}{n}, \qquad f_a = \frac{1}{(1-x)^k},$$

$$a_n = n^2, \qquad f_a = \frac{x(1+x)}{(1-x)^3},$$

$$a_n = n^3, \qquad f_a = \frac{x(x+2)^2-3x}{(1-x)^4},$$

$$a_n = \begin{cases} 0, & n=0, \\ 1/n, & n>0, \end{cases} \qquad f_a = -\ln(1-x),$$

$$a_n = \frac{1}{n!}, \qquad f_a = e^x.$$

Zastosujemy poznany powyżej system skrótów do rozwiązywania równań rekurencyjnych. Zacznijmy od prostego przykładu. Przypomnijmy, że liczby Fibonacciego (por. § 10, rozdz. 1) definiujemy przez zależności

$$a_0 = a_1 = 1, \qquad a_{n+2} = a_{n+1} + a_n.$$

Niech ciąg $\boldsymbol{a} = \langle a_n \rangle_{n=0}^{\infty}$ będzie ciągiem wyznaczonym przez powyższe warunki. Oznaczając $f = f_{\boldsymbol{a}}$, i przyjmując $c_n = a_{n+2}$ mamy – zgodnie z twierdzeniem 5.1(b) – $f_{\boldsymbol{c}} = x^{-2}(f-(a_0+a_1 x))$. Podobnie dla $b_n = a_{n+1}$ mamy $f_{\boldsymbol{b}} = x^{-1}(f-a_0)$. Równość $\boldsymbol{c} = \boldsymbol{a}+\boldsymbol{b}$ jest równoważna równości $f_{\boldsymbol{c}} = f_{\boldsymbol{a}} + f_{\boldsymbol{b}}$, a zatem

$$\frac{1}{x^2}\left(f-(a_0+a_1 x)\right) = \frac{1}{x}\left(f-a_0\right)+f.$$

Ale $a_0 = a_1 = 1$. Wobec tego

$$\left(\frac{1}{x^2}-\frac{1}{x}-1\right)f = \frac{1+x}{x^2}-\frac{1}{x} = \frac{1}{x^2},$$

czyli

$$f = \frac{1}{1-x-x^2}.$$

Wystarczy teraz znaleźć rozwinięcie w szereg wyrażenia $1/(1-x-x^2)$, aby znaleźć ciąg liczb Fibonacciego. W tym celu rozłożymy je do postaci

$$\frac{1}{1-x-x^2} = \frac{1}{\left(1-\frac{1}{2}(1+\sqrt{5})x\right)\left(1-\frac{1}{2}(1-\sqrt{5})x\right)} =$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)\frac{1}{1-\frac{1}{2}(1+\sqrt{5})x} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)\frac{1}{1-\frac{1}{2}(1-\sqrt{5})x}.$$

Korzystając z twierdzenia 5.1(c) mamy

$$\frac{1}{1-cx} = \sum_{n=0}^{\infty} c^n x^n,$$

a więc

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} \left[\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n\right]x^n =$$

$$= \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right]x^n,$$

czyli

$$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right]$$

(por. § 10, rozdz. 1). Oczywiście, gdybyśmy znali powyższy wzór, to udowodnienie – przez indukcję – że jest to rozwiązanie równania Fibonacciego jest nader proste. Jednakże dzięki zastosowaniom funkcji tworzących mogliśmy znaleźć rozwiązanie bez zgadywania, co w inny sposób byłoby raczej kłopotliwe. Powyższa technika może być zastosowana do rozwiązywania liniowych równań różnicowych, czyli do równań postaci

$$c_1 a_n + c_2 a_{n+1} + \ldots + c_k a_{n+k} = b_n, \qquad n = 0, 1, \ldots,$$

gdzie $a_0, \ldots, a_k$ są znane, a $\langle b_n \rangle_{n=0}^{\infty}$ jest danym ciągiem. Przyjmując mianowicie $d_n^1 = a_{n+1}, \ldots, d_n^k = a_{n+k}$ mamy

$$f_{d^1} = \frac{1}{x}(f_a - a_0), \qquad \ldots \qquad f_{d^k} = \frac{1}{x^k}(f_a - (a_0 + a_1 x + \ldots + a_{k-1} x^{n-1})).$$

Otrzymujemy stąd równość

$$c_1 f_a + c_2 \frac{1}{x}(f_a - a_0) + \ldots + c_k \frac{1}{x^k}(f_a - (a_0 + a_1 x + \ldots + a_{k-1} x^{k-1})) = f_b,$$

czyli

$$\left(c_1 + c_2 \frac{1}{x} + \ldots + c_k \frac{1}{x^k}\right) f_a - \frac{w(x)}{x^k} = f_b,$$

gdzie $w(x)$ jest wielomianem stopnia co najwyżej k. Przyjmując $v(x) = c_1 x^k + c_2 x^{k-1} + \ldots + c_k$ mamy

$$f_a = \frac{x^k f_b + w(x)}{v(x)}.$$

Zauważmy, że rozwiązalność naszego równania wymaga, by $c_k \neq 0$, wtedy bowiem szereg $v(x)$ jest odwracalny.

Rozwiążmy dla przykładu równanie $a_{n+1}-2a_n = n$, $a_0 = 1$. Zgodnie z powyższym mamy

$$\frac{1}{x}(f_a-1)-2f_a = \frac{x}{(1-x)^2}.$$

(Pamiętamy, że dla $b_n = n$, $f_a = x/(1-x)^2$.) Wobec tego

$$f_a \cdot \frac{1-2x}{x} - \frac{1}{x} = \frac{x}{(1-x)^2},$$

czyli

$$f_a = \frac{x}{1-2x}\left(\frac{x}{(1-x)^2}+\frac{1}{x}\right) = \frac{x^2+(1-x)^2}{(1-2x)(1-x)^2}.$$

Rozkładając prawą stronę równości na ułamki proste otrzymujemy

$$\frac{2}{1-2x} - \frac{1}{(1-x)^2},$$

a więc, zgodnie z naszym katalogiem,

$$a_n = 2 \cdot 2^n - \binom{n+1}{n} = 2^{n+1}-(n+1), \qquad a_0 = 1.$$

§ 6. Zastosowania eksponencjalnych funkcji tworzących, wzór eksponencjalny

W paragrafie tym będziemy stosowali eksponencjalne szeregi formalne do problemów numeracji związanych z podziałami zbiorów skończonych. Zauważmy najpierw, rozważając na przykład podziały zbioru czteroelementowego, że krata podziałów nie ma własności dwumianowej i zatem metody z paragrafu 2 nie są przydatne w zagadnieniach numeracji związanych z Π_n. Wypracujemy inne metody także związane z szeregami formalnymi i podamy liczne zastosowania.

Najpierw zauważmy, iż istnieje naturalne włożenie rodziny Π_n podziałów zbioru $\{1, \ldots, n\}$ w rodzinę Π_m dla $m \geqslant n$. Mianowicie podziałowi σ z Π_n przyporządkowujemy podział σ' złożony z bloków podziału σ oraz jeszcze jednego bloku złożonego z liczb $\{n+1, \ldots, m\}$. Przyporządkowanie to jest wierne w tym sensie, że podział σ jest drobniejszy od podziału π wtedy i tylko wtedy, gdy podział σ' jest drobniejszy od podziału π'.

Przejdźmy z tą konstrukcją „do nieskończoności" zanurzając równocześnie wszystkie kraty Π_n, $n \in N$, w kratę podziałów zbioru nieskończonego N.

Wyróżnijmy pewną klasę podziałów zbioru $\boldsymbol{N}$, którą oznaczamy Π. Mianowicie π jest elementem Π wtedy i tylko wtedy gdy:

(1) π ma skończoną liczbę bloków,

(2) dokładnie jeden z bloków podziału π jest nieskończony,

(3) każda liczba z nieskończonego bloku jest większa od wszystkich liczb należących do bloków skończonych.

Teraz już widać, że Π jest właśnie ową „granicą" zanurzeń kolejnych Π_n. Nie wnikając w algebraiczne aspekty sprawy zauważmy, że dla każdego podziału zbioru n-elementowego znajdziemy w Π podział π, który na odcinku $[1, n]$ indukuje podział izomorficzny z zadanym.

Możemy pokazać nawet więcej. A mianowicie to, że Π jest zbiorem częściowo uporządkowanym, który jest lokalnie skończony. Ponadto każdą kratę podziałów Π_n można utożsamiać – poprzez skonstruowane powyżej zanurzenie – z pewnym odcinkiem zbioru Π. Wreszcie, zbiór uporządkowany Π nie ma własności dwumianowej. Rolę używanych uprzednio funkcji przesuwalnych będą pełniły zdefiniowane dalej funkcje multyplikatywne.

Typem odcinka $[\sigma, \pi]$ nazywamy ciąg $\langle k_1, k_2, \ldots \rangle$ taki, że dla każdego $j \in \boldsymbol{N}$ w podziale π jest k_j skończonych bloków będących sumą j bloków podziału σ. Ciąg $\langle k_n \rangle_{n=1}^{\infty}$ jest oczywiście od pewnego miejsca stały i równy zeru.

Funkcję f z algebry incydencji $\mathscr{A}(\Pi)$ nazwiemy *multyplikatywną*, jeśli istnieje ciąg $\langle a_n \rangle_{n=1}^{\infty}$ taki, że ilekroć typem odcinka $[\sigma, \pi]$ jest $\langle k_1, k_2, \ldots \rangle$, to

$$f(\sigma, \pi) = \prod_{j=1}^{\infty} a_j^{k_j}.$$

Skoro ciąg $\langle k_n \rangle_{n=1}^{\infty}$ jest od pewnego miejsca stały i równy zeru, to definicja nasza jest poprawna.

Jak się niebawem okaże, klasa funkcji multyplikatywnych jest nader ważna w zastosowaniach. Zauważmy najpierw następujący fakt.

LEMAT 6.1. *Na to, by odcinek $[\sigma, \pi]$ był typu $\langle k_n \rangle_{n=1}^{\infty}$, potrzeba i wystarcza, by był on izomorficzny z iloczynem*

$$\Pi_1^{k_1} \times \Pi_2^{k_2} \times \ldots$$

Dowód tego faktu został w istocie podany w dowodzie lematu 3.9 z rozdz. 2 (w przypadku $\sigma, \pi \in \Pi_n$, ale zgodnie z naszymi uwagami nie jest to istotne zmniejszenie ogólności). □

LEMAT 6.2. *Splot funkcji multyplikatywnych jest funkcją multyplikatywną.*

Dowód. Wystarczy skorzystać – odpowiednią liczbę razy – z następującego prostego faktu: Jeśli $f \in \mathscr{A}(\boldsymbol{P})$, $g \in \mathscr{A}(\boldsymbol{Q})$, to definiując

$$(f \times g)(\langle x, x' \rangle, \langle y, y' \rangle) = f(x, y) \cdot g(x', y')$$

mamy

$$(g \times g) * (f' \times g') = (f * f') \times (g * g'). \quad \square$$

Rodzinę funkcji multyplikatywnych oznaczamy przez $M(\Pi)$.

Nim przejdziemy do dalszych rozważań zauważmy, że funkcja ζ jest multyplikatywna i wyznaczona przez ciąg złożony z samych jedynek. Także funkcja δ jest multyplikatywna i wyznaczona przez ciąg $\langle 1, 0, 0, \ldots \rangle$.

Wykażemy teraz zasadnicze twierdzenie tego paragrafu. Wnioski z tego twierdzenia, w szczególności „wzór eksponencjalny", mają liczne zastosowania w zagadnieniach zliczania.

Niech $f \in M(\Pi)$ i niech ciąg $\langle a_n \rangle_{n=1}^{\infty}$ wyznacza funkcję f. Funkcji f przyporządkowujemy szereg formalny F_f określony następująco

$$F_f = \sum_{n=1}^{\infty} \frac{a_n}{n!} x^n.$$

Definicja ta jest poprawna, gdyż odpowiedniość pomiędzy funkcjami i ciągami jest oczywiście wzajemnie jednoznaczna. Zauważmy, że skoro wyraz wolny szeregu F_f jest zerem, to może on być podstawiony do innego szeregu w miejsce zmiennej (por. § 1).

Zachodzi następujące „twierdzenie o antyizomorfizmie".

TWIERDZENIE 6.3 (Doubilet, Rota i Stanley [1]). *Przekształcenie przypisujące funkcji multyplikatywnej $f \in M(\Pi)$, wyznaczonej przez ciąg $\langle a_n \rangle_{n=1}^{\infty}$, eksponencjalny szereg formalny $F_f = \sum_{n=1}^{\infty} \frac{a_n}{n!} x^n$ odwzorowuje wzajemnie jednoznacznie zbiór funkcji multyplikatywnych $M(\Pi)$ z działaniem splotu na zbiór eksponencjalnych szeregów formalnych o wyrazie wolnym równym zeru z działaniem podstawienia. Ponadto*

$$F_{f*g}(x) = F_g(F_f(x)).$$

(Uwaga! Zmiana kolejności działań.)

Dowód. Dzięki uwagom poprzedzającym twierdzenie pozostało nam jedynie do wykazania, że $F_{f*g}(x) = F_g(F_t(x))$. Zbadajmy współczynniki przy potęgach zmiennej x w wyrażeniach stojących po obu stronach równości

$$F_g(F_f(x)) = \sum_{n=1}^{\infty} \frac{b_n}{n!} \left(\sum_{n=1}^{\infty} \frac{a_m}{m!} x^m \right)^n = \sum_{n=1}^{\infty} \frac{b_n}{n!} \left(\sum_{\langle t_1, \ldots, t_n \rangle \in N^n} \frac{a_{t_1} \ldots a_{t_n}}{t_1! \ldots t_n!} x^{t_1 + \ldots + t_n} \right).$$

Będziemy teraz dążyli do zmiany porządku sumowania tak, by pogrupować odpowiednio potęgi zmiennej. Otóż dla każdego ciągu $\langle t_1, \ldots, t_n \rangle \in N^n$ takiego, że $t_1 + \ldots + t_n = k$ we współczynniku przy x^k mamy składnik

$$\frac{b_n}{n!} \cdot \frac{a_{t_1} \ldots a_{t_n}}{t_1! \ldots t_n!}.$$

Grupując odpowiednio i biorąc pod uwagę permutacje ciągów otrzymujemy

$$F_g(F_f(x)) = \sum_{n=1}^{\infty} h_n \frac{x^n}{n!},$$

gdzie

$$h_n = \sum \frac{n!}{1!^{s_1} \ldots n!^{s_n} s_1! \ldots s_n!} a_1^{s_1} \ldots a_n^{s_n} b_k.$$

Sumowanie to rozciąga się po wszystkich ciągach $s_1, \ldots, s_n$ takich, że

$$\sum_{j=1}^{n} j s_j = n \quad \text{oraz} \quad k = \sum_{j=1}^{n} s_j.$$

Pozostaje zatem zbadać współczynniki szeregu $F_{f*g}(x)$. Na początek zbadajmy jak zależą wyrazy ciągu $\langle a_n \rangle_{n=1}^{\infty}$ od wyznaczonej przezeń funkcji f. Otóż $a_n = f(\sigma, \pi)$, gdzie typem odcinka $[\sigma, \pi]$ jest ciąg $\langle k_1, k_2, \ldots \rangle$, gdzie $k_1 = 0, \ldots, k_{n-1} = 0, k_n = 1, k_{n+1} = 0, \ldots$ Oznacza to, że dla odnalezienia szukanego współczynnika musimy znaleźć wartość splotu $f * g$ na tym odcinku. Odcinek ten jest izomorficzny z kratą Π_n. Zanurzając Π_n w Π i utożsamiając Π_n z obrazem stwierdzamy, iż poszukujemy liczby

$$\sum_{\tau \in \Pi_n} f(\mathbf{0}, \tau) \cdot g(\tau, \mathbf{1}),$$

gdzie przez **0** i **1** oznaczyliśmy zero i jedynkę kraty Π_n. Najpierw zauważmy, że $g(\tau, \mathbf{1})$ jest równe b_k ilekroć τ jest podziałem na k bloków. Naszym współczynnikiem jest zatem

$$\sum_{\tau \in \Pi_n} f(\mathbf{0}, \tau) b_{|\tau|}.$$

Suma ta jest równa

$$\sum_{\tau \in \Pi_n} a_1^{s_1} \ldots a_n^{s_n} b_{|\tau|},$$

gdzie s_j jest liczbą bloków liczności j w podziale τ, zaś $|\tau| = \sum_{j=1}^{n} s_j$.

Szukamy zatem liczby podziałów dających współczynnik

$$a_1^{s_1} \ldots a_n^{s_n} b_{s_1 + \ldots + s_n}.$$

Tych jest zaś

$$\frac{n!}{1!^{s_1} s_1! \, 2!^{s_2} s_2! \ldots n!^{s_n} s_n!}$$

(por. rozdz. 1, twierdzenie 8.2). Tak więc współczynnikiem tym jest

$$\sum_{\substack{1a_1+\ldots+na_n=n\\ a_1+\ldots+a_n=k}} \frac{n!}{1!^{s_1}s_1!\ldots n!^{s_n}s_n!}\, a_1^{s_1}\ldots a_n^{s_n} b_k.$$

Ta ostatnia liczba to dokładnie h_n. To kończy dowód. □

WNIOSEK 6.4. *Jeżeli f jest funkcją multyplikatywną, która jest odwracalna w algebrze $\mathscr{A}(\Pi)$, to funkcja f^{-1} jest też multyplikatywna. Innymi słowy: zbiór funkcji $f \in M(\Pi)$ takich, że $f(\sigma, \sigma) \neq 0$ dla $\sigma \in \Pi$, wraz ze splotem tworzy grupę.*

Dowód. Niech $f \in M(\Pi)$ będzie funkcją wyznaczoną przez ciąg $\langle a_n \rangle_{n=1}^{\infty}$. Z ogólnych własności algebry incydencji $\mathscr{A}(\Pi)$ wiadomo, że funkcja f jest odwracalna wtedy i tylko wtedy, gdy $a_1 = f(\sigma, \sigma)$, dla każdego $\sigma \in \Pi$, jest różne od zera (por. rozdz. 2, twierdzenie 1.2). Niech $F(x) = \sum_{n=1}^{\infty} a_n x^n/n!$. Będziemy szukali takiego szeregu $G(x) = \sum_{n=1}^{\infty} b_n x^n/n!$, aby

$$G(F(x)) = F_\delta(x) = x.$$

Skoro

$$G(F(x)) = \frac{b_1}{1!}F(x) + \frac{b_2}{2!}F^2(x) + \frac{b_3}{3!}F^3(x) + \ldots = x,$$

to odszukanie ciągu $\langle b_n \rangle_{n=1}^{\infty}$ sprowadza się do rozwiązania układu równań liniowych. W równaniu powstałym przez porównanie współczynników przy x^k po obu stronach równości występują niewiadome b_i tylko dla $i \leqslant k$. Ponadto współczynnik przy b_k jest równy $a_1^k/k!$, a więc jest różny od zera. Oznacza to, że układ ten zawsze można rozwiązać metodą eliminacji. Rozważając multyplikatywną funkcję g wyznaczoną przez ciąg $\langle b_n \rangle_{n=1}^{\infty}$ otrzymujemy zatem $F_{f*g}(x) = F_g(F_f(x)) = G(F(x)) = F_\delta$. Wobec tego $f * g = \delta$, a ponieważ funkcja f jest odwracalna, więc $g = f^{-1}$. Zatem $f^{-1} \in M(\Pi)$. □

Jak zauważyliśmy uprzednio, funkcja ζ w kracie Π jest funkcją multyplikatywną. Wobec powyższego ta sama własność przysługuje funkcji $\mu = \zeta^{-1}$. Odszukamy szereg $M(x) = F_\mu(x)$. Ponieważ $F_\zeta(x) = \sum_{n=1}^{\infty} x^n/n! = e^x - 1$, więc $M(x)$ jest jedynym szeregiem takim, że $M(0) = 0$ i

$$(\exp M(x)) - 1 = x.$$

Stosując do obu stron operator D i korzystając ze wzoru na różniczkowanie szeregu złożonego (zad. 8) otrzymujemy

$$(\exp M(x))\, DM(x) = 1.$$

Jednakże $\exp M(x) = 1+x$, a więc

$$DM(x) = \frac{1}{1+x} = \sum_{n=1}^{\infty} (-x)^n.$$

Uwzględniając fakt, że $M(0) = 0$ i „formalnie całkując" znajdujemy

$$M(x) = \sum_{n=1}^{\infty} (-1)^{n-1} \frac{x^n}{n} = \sum_{n=1}^{\infty} (-1)^{n-1}(n-1)!\,\frac{x^n}{n!}.$$

Oznacza to, że $(-1)^{n-1}(n-1)!$ jest wartością funkcji Möbiusa na każdym odcinku $[\sigma, \pi]$ o typie równym $\langle k_1, k_2, \ldots\rangle$, gdzie $k_n = 1$ i $k_m = 0$, dla $m \neq n$. W szczególności

$$\mu_{\Pi_n}(\mathbf{0}, \mathbf{1}) = (-1)^{n-1}(n-1)!.$$

Pokazaliśmy zatem inny dowód wyniku Schutzenbergera [1] i Roty [2] (por. rozdz. 2, tw. 3.10).

Z oczywistych względów szereg $M(x) = F_\mu(x) = \sum_{n=1}^{\infty} -(-x)^n/n$ jest oznaczany przez $\ln(1+x)$. Szereg ten z funkcją zespoloną $\ln(1+z)$ dzieli jeszcze inne własności poza podobnym rozwinięciem. Zachodzi mianowicie następujący, nader użyteczny w zastosowaniach fakt.

Lemat 6.5. *Niech H będzie szeregiem formalnym i niech $H(0) = 0$. Wówczas*

$$\exp(\ln(1+H))-1 = \ln(\exp H) = H.$$

Dowód. Rozważmy funkcję multyplikatywną h taką, że $H = F_h$. Wówczas

$$\exp(\ln(1+H))-1 = F_\zeta(F_\mu(F_h)) = F_{h*\mu*\zeta} = F_h = H.$$

Podobnie dowodzimy drugiej równości korzystając z tego, że

$$\ln(\exp H) = \ln(1+(\exp H-1)). \quad \square$$

Nim przejdziemy do bezpośrednich zastosowań do problemów zliczania, znajdziemy eksponencjalną funkcję tworzącą dla liczb Bella B_n (por. rozdz. 1, § 8). Przypomnijmy, że $B_n = |\Pi_n|$. Na podstawie rozważań z § 2 wiemy, że $\zeta * \zeta(a, b)$ jest licznością odcinka $[a, b]$. Mamy zatem

$$\zeta_{\Pi_n} * \zeta_{\Pi_n}(\mathbf{0}, \mathbf{1}) = B_n.$$

Zanurzając Π_n w Π i pamiętając, iż $F_\zeta = e^x - 1$ mamy

$$\sum_{n=1}^{\infty} \frac{B_n}{n!} x^n = \exp(e^x-1)-1,$$

ponieważ $F_{\zeta*\zeta} = F_\zeta(F_\zeta)$.

Przyjmując $B_0 = 1$ otrzymujemy znany wynik:

TWIERDZENIE 6.6 (Bell). *Eksponencjalną funkcję tworzącą dla liczb Bella jest* $\exp(e^x-1)$. *Wobec tego*

$$B_n = [D^n(\exp(e^x-1))]_{x=0}. \quad \square$$

Uzyskamy teraz dalsze informacje o ciągu $\langle B_n\rangle_{n=0}^{\infty}$. Skoro

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} x^n = \exp(e^x-1),$$

to różniczkując stronami otrzymujemy

$$\sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} x^n = \exp(e^x-1)\cdot e^x = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n \cdot \sum_{n=0}^{\infty} \frac{x^n}{n!}.$$

Prawa strona naszej równości, na mocy wzoru Cauchy'ego, jest równa

$$\sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} \frac{B_j}{j!}\cdot\frac{1}{(n-j)!}\right)x^n = \sum_{n=0}^{\infty} \left(\sum_{j=0}^{n} \binom{n}{j} B_j\right)\frac{x^n}{n!}.$$

Z porównania współczynników w poprzedniej równości wynika, że

$$B_{n+1} = \sum_{j=0}^{n} \binom{n}{j} B_j,$$

co daje rekurencyjną zależność dla liczb Bella, otrzymaną innym sposobem w rozdz. 1 (por. twierdzenie 8.6).

Wreszcie, przechodząc do szeregów zmiennej zespolonej, mamy

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n = \exp(e^z-1) = \frac{1}{e}\exp e^z = \frac{1}{e}\sum_{n=0}^{\infty} \frac{e^{nz}}{n!} =$$

$$= \frac{1}{e}\sum_{n=0}^{\infty} \frac{1}{n!}\sum_{k=0}^{\infty} \frac{(nz)^k}{k!} = \frac{1}{e}\sum_{n=0}^{\infty} \frac{1}{n!}\sum_{k=0}^{\infty} \frac{n^k}{k!} z^k.$$

Zmieniając porządek sumowania otrzymujemy

$$\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n = \frac{1}{e}\sum_{n=0}^{\infty} \left(\sum_{k=0}^{\infty} \frac{k^n}{k!}\right)\frac{z^n}{n!}.$$

Uzyskujemy stąd natychmiast klasyczny rezultat:

TWIERDZENIE 6.7 (Dobinski [1], 1877).

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty} \frac{k^n}{k!}. \quad \square$$

Inny dowód twierdzenia 6.7 można podać korzystając z faktu, iż liczby $D_n = \frac{1}{e}\sum_{k=0}^{\infty} \frac{k^n}{k!}$ **spełniają zależności** $D_0 = 1$ **oraz** $D_{n+1} = \sum_{k=0}^{n} \binom{n}{k} D_k$. **Stąd** $B_n = D_n$, **przez indukcję.**

Podobnych metod możemy użyć dla znalezienia funkcji tworzącej dla liczb

Stirlinga drugiego rodzaju. Przypomnijmy, że $S(n, m)$ jest liczbą podziałów zbioru n-elementowego na dokładnie m bloków. To że podział π ma dokładnie m bloków oznacza, że odcinek $[\pi, \mathbf{1}]$ ma typ odcinka Π_m kraty Π. Określmy zatem h_n wzorem

$$h_n(\sigma, \pi) = \begin{cases} 1, & \text{jeśli odcinek } [\sigma, \pi] \text{ ma typ odcinka } \Pi_m, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Oczywiście $S(n, m) = \sum_{\pi \in \Pi_n} \zeta(\mathbf{0}, \pi) \cdot h_m(\pi, \mathbf{1})$, a więc $S(n, m) = (\zeta_{\Pi_n} * h_m)(\mathbf{0}, \mathbf{1})$.

Łatwo widzieć, iż h_n jest funkcją multyplikatywną i że jest ona wyznaczona przez ciąg $(0, 0, \ldots, 1, 0, \ldots)$, który ma dokładnie jedną jedynkę na m-tym miejscu. Stąd $F_{h_m} = \frac{x^m}{m!}$. Natomiast szereg $\sum_{n=1}^{\infty} \frac{S(n, m)}{n!} x^n$ jest postaci

$$F_{\zeta * h_m} = F_{h_m}(F_\zeta) = \frac{(e^x - 1)^m}{m!} = \frac{1}{m!} \sum_{j=0}^{m} \binom{n}{j} e^{jx} (-1)^{n-j}.$$

Mamy więc

$$\sum_{n=1}^{\infty} \frac{S(n, m)}{n!} x^n = \frac{1}{m!} \sum_{j=0}^{m} (-1)^{n-j} \binom{m}{j} e^{jx}.$$

Obliczając wartość w punkcie $x = 0$ r-tej pochodnej wyrażeń stojących po obu stronach tej równości otrzymujemy

$$S(r, m) = \frac{1}{m!} \sum_{j=0}^{m} (-1)^{m-j} \binom{m}{j} j^r$$

(por. rozdz. 1 tw. 8.4).

Przejdziemy teraz do zastosowań twierdzenia 6.3. Przyjmując za g w twierdzeniu 6.3 funkcję stale równą 1 otrzymujemy następujący wniosek.

WNIOSEK 6.8 („wzór eksponencjalny"). *Niech $f: \mathbf{N} \to \mathbf{C}$, niech F będzie szeregiem formalnym $\sum_{n=1}^{\infty} f(n) \frac{x^n}{n!}$, funkcja zaś $h: \mathbf{N} \to \mathbf{C}$ niech będzie dana wzorem*

$$h(n) = \sum_{\pi \in \Pi_n} (f(1))^{a_1} \ldots (f(n))^{a_n},$$

gdzie sumowanie rozciąga się na wszystkie podziały zbioru n-elementowego, a ciąg $\langle a_1, \ldots, a_n \rangle$ oznacza typ podziału π.

Jeżeli $H(x) = \sum_{n=1}^{\infty} h(n) \frac{x^n}{n!}$, to

$$H(x) = \exp F(x) - 1.$$

Dowód. Szereg odpowiadający multyplikatywnej funkcji g jest równy $e^x - 1$. □

Gdy $f \equiv 1$, wówczas $F(x) = e^x - 1$ i prawa strona wzoru eksponencjalnego przyjmuje postać $\exp(e^x - 1) - 1$. Natomiast z drugiej strony $H(x) = \sum_{n=1}^{\infty} h(n) \frac{x^n}{n!}$, przy czym $h(n) = \sum_{\pi \in \Pi_n} 1^{a_1} \dots 1^{a_n} \cdot 1 = |\Pi_n| = B_n$. Tak więc otrzymaliśmy inny dowód twierdzenia Bella.

Podamy poniżej klasyczne zastosowania wzoru eksponencjalnego do problemów zliczania.

Permutacje spełniające warunek $\sigma^m = 1$ (1 oznacza tu permutację identycznościową). Niech $m \in N$. Znajdziemy eksponencjalną funkcję tworzącą H_m dla funkcji h_m, gdzie

$h_m(n)$ = liczność zbioru tych permutacji σ zbioru $\{1, \dots, n\}$, dla których $\sigma^m = 1$ ($h_m(0) = 1$).

Niech $n \neq 0$. Podamy metodę konstrukcji wszystkich permutacji σ zbioru $\{1, \dots, n\}$ spełniających warunek $\sigma^m = 1$. Warunek ten oznacza, że długość każdego cyklu permutacji σ musi być dzielnikiem liczby m. Stąd też permutacja σ taka, że $\sigma^m = 1$, powstaje w następujący sposób. Dzielimy zbiór $\{1, \dots, n\}$ na bloki, z których każdy ma liczność będącą dzielnikiem liczby m. Następnie wewnątrz każdego z bloków podziału ustalamy porządek cykliczny. Jeśli blok liczy d elementów, to istnieje dokładnie $(d-1)!$ takich porządków. Przyjmijmy

$$f(d) = \begin{cases} (d-1)!, & \text{jeśli } d|m, \\ 0, & \text{w przeciwnym przypadku.} \end{cases}$$

Łatwo widzieć, iż zachodzi

$$h_m(n) = \sum_{\pi \in \Pi_n} f(1)^{a_1} \dots f(n)^{a_n}$$

(gdzie $\langle a_1, \dots, a_n \rangle$ jest typem podziału π).

Istotnie, jeśli permutacja π ma jakikolwiek cykl elementarny długości d, nie będącej dzielnikiem liczby m, to nie zostanie w ten sposób policzona. W przeciwnym zaś razie zostanie policzona dokładnie jeden raz.

Zastosujmy teraz wzór eksponencjalny. Lewa strona przyjmuje postać $H_m(x) - 1$ ($h(0)$ zostało bowiem określone jako 1), prawa zaś strona postać $e^{F(x)} - 1$, gdzie $H_m(x) = \sum_{n=1}^{\infty} h_m(n) \frac{x^n}{n!}$ i $F(x) = \sum_{n=1}^{\infty} f(n) \frac{x^n}{n!}$. Wystarczy zatem znaleźć $F(x)$. To jednak jest łatwe:

$$F(x) = \sum_{d=1}^{\infty} f(d) x^d/d = \sum_{d|m} (d-1)!\, x^d/d! = \sum_{d|m} x^d/d.$$

Tak więc ostatecznie $H_m(x) = \exp(\sum_{d|m} x^d/d)$ (por. Chowla, Herstein i Scott [1]).

W szczególności dla $m = 2$, $H_2(x) = \exp(x + x^2/2)$.

Grafy, których składowe spójne są cyklami, krawędziami lub wierzchołkami izolowanymi. Będziemy szukać eksponencjalnej funkcji tworzącej K dla funkcji k, gdzie

$k(n) =$ liczba grafów Γ o zbiorze wierzchołków $\{1, \ldots, n\}$ takich, że każda składowa spójna Γ jest cyklem, krawędzią lub wierzchołkiem izolowanym $(k(0) = 1)$.

Niech f będzie funkcją określoną na N jak następuje

$$f(n) = \begin{cases} 1 & \text{dla } n = 1, 2, \\ (n-1)!/2 & \text{dla } n \geqslant 3. \end{cases}$$

Podamy teraz metodę konstrukcji wszystkich grafów (niezorientowanych) na zbiorze $\{1, \ldots, n\}$ spełniających warunek określony w problemie. Aby skonstruować taki graf, należy wybrać podział $\pi = \{B_1, \ldots, B_k\}$ naszego zbioru i w każdym bloku podziału o liczności co najmniej 3 określić porządek cykliczny. Przy tym, ze względu na to, iż rozważamy grafy niezorientowane, „zlepiamy" za każdym razem 2 porządki. Łatwo widzieć, że

$$k(n) = \sum_{\pi \in \Pi_n} f(1)^{a_1} \ldots f(n)^{a_n}.$$

Stosujemy więc wzór eksponencjalny

$$K(x) - 1 = e^{F(x)} - 1,$$

gdzie

$$F(x) = \sum_{n=1}^{\infty} f(n) x^n/n!.$$

Mamy więc

$$F(x) = x + x^2/2 + \sum_{n=3}^{\infty} \tfrac{1}{2}(n-1)!\, x^n/n! = x + x^2/2 + \tfrac{1}{2} \sum_{n=3}^{\infty} x^n/n$$

$$= x/2 + x^2/4 + \tfrac{1}{2} \sum_{n=1}^{\infty} x^n/n = x/2 + x^2/4 - \tfrac{1}{2} \ln(1-x).$$

Stąd $K(x) = \exp\big(x/2 + x^2/4 - \tfrac{1}{2}\ln(1-x)\big)$.

Wykorzystując teraz, między innymi, lemat 6.5 i zadanie 10, ostatecznie otrzymujemy

$$K(x) = (1-x)^{-1/2} \exp(x/2 + x^2/4).$$

Grafy spójne. Będziemy rozważali eksponencjalną funkcję tworzącą dla funkcji $f\colon N \to N$, gdzie $f(n)$ jest liczbą grafów spójnych na zbiorze $\{1, \ldots, n\}$.

Wszystkich grafów na zbiorze $\{1, \ldots, n\}$ jest oczywiście tyle, ile zbiorów złożonych z par elementów zbioru $\{1, \ldots, n\}$, a więc $2^{\binom{n}{2}}$.

Podamy teraz metodę konstrukcji wszystkich grafów w zbiorze $\{1, \ldots, n\}$. Aby skonstruować graf Γ, należy wybrać podział $\pi = \{B_1, \ldots, B_k\}$. Zbiory $B_1, \ldots, B_k$ określą składowe spójne grafu Γ. Następnie w każdym bloku B_i wybieramy graf spójny na elementach zbioru B_i. Zachodzi więc równość

$$2^{\binom{n}{2}} = \sum_{\pi \in \Pi_n} f(1)^{a_1} \ldots f(n)^{a_n}.$$

Stosujemy wzór eksponencjalny otrzymując

$$\sum_{n=1}^{\infty} 2^{\binom{n}{2}} x^n/n! = e^{F(x)} - 1,$$

gdzie $F(x) = \sum_{n=1}^{\infty} f(n) x^n/n!$. Mamy zatem

$$\sum_{n=0}^{\infty} 2^{\binom{n}{2}} x^n/n! = e^{F(x)}.$$

(Zauważmy, że szereg $\sum_{n=0}^{\infty} 2^{\binom{n}{2}} z^n/n!$ ma promień zbieżności 0.)

Wykazaną powyżej zależność użyjemy do znalenienia wzoru rekurencyjnego dla funkcji f.

Dowodzimy najpierw następującego lematu:

LEMAT 6.9. *Jeśli*

$$G(x) = \sum_{n=0}^{\infty} g(n) x^n, \qquad H(x) = \sum_{n=1}^{\infty} h(n) x^n$$

oraz $G(x) = e^{H(x)}$, *to*

$$h(n) = g(n) - \frac{1}{n} \sum_{k=1}^{n-1} kh(k) g(n-k).$$

Dowód. Mamy $H(x) = \ln G(x)$. Zatem $H'(x) = G'(x)(G(x))^{-1}$, a więc $G'(x) = H'(x) G(x)$. Stąd

$$\sum_{n=0}^{\infty} ng(n) x^{n-1} = \sum_{n=1}^{\infty} nh(n) x^{n-1} \cdot \sum_{n=0}^{\infty} g(n) x^n.$$

Stosując wzór Cauchy'ego do prawej strony równości i porównując współczynniki otrzymujemy po elementarnych przekształceniach tezę lematu. □

Stosując powyższy lemat do funkcji $g(n) = 2^{\binom{n}{2}}/n!$, $h(n) = f(n)/n!$ otrzymujemy:

$$f(n)/n! = 2^{\binom{n}{2}}/n! - \frac{1}{n} \sum_{k=1}^{n-1} k \frac{2^{\binom{k}{2}} f(n-k)}{k!(n-k)!}.$$

Stąd

$$f(n) = 2^{\binom{n}{2}} - (n-1)! \sum_{k=1}^{n-1} \frac{2^{\binom{k}{2}} f(n-k)}{(k-1)!(n-k)!},$$

a więc

$$f(n) = 2^{\binom{n}{2}} - \sum_{k=1}^{n-1} \binom{n-1}{k-1} 2^{\binom{k}{2}} f(n-k).$$

Podstawiając $n-k$ zamiast k, otrzymujemy

$$f(n) = 2^{\binom{n}{2}} - \sum_{k=1}^{n-1} \binom{n-1}{k-1} 2^{\binom{n-k}{2}} f(k).$$

Funkcje idempotentne. Będziemy szukali eksponencjalnej funkcji tworzącej I dla funkcji i określonej jak następuje:

$i(n) =$ liczność zbioru funkcji idempotentnych na zbiorze $\{1, \ldots, n\}$.

(Funkcja g nazywa się *idempotentna*, jeśli $g = g^2$.) Przyjmujemy $i(0) = 1$.

Zauważmy, że g jest idempotentna wtedy i tylko wtedy, gdy dla każdego j, $g^{-1}(j)$ jest zbiorem pustym, lub też $j \in g^{-1}(j)$. Istotnie, jeśli $g^{-1}(j)$ jest niepusty i $r \in g^{-1}(j)$, to $g(r) = j$ i $g(g(r)) = g(r)$, czyli $g(j) = j$, a więc $j \in g^{-1}(j)$.

Niech f będzie funkcją określoną na N jak następuje: $f(n) = n$.

Podamy teraz metodę konstrukcji wszystkich funkcji idempotentnych na zbiorze $\{1, \ldots, n\}$. Aby skonstruować funkcję idempotentną, należy – zgodnie z powyższymi uwagami – obrać podział $\{B_1, \ldots, B_k\}$ naszego zbioru i przekształcić każdy z bloków na jeden z jego elementów. Mamy oczywiście $|B|$ możliwości, a zatem łatwo widzieć, iż

$$i(n) = \sum_{\pi \in \Pi_n} f(1)^{a_1} \ldots f(n)^{a_n}.$$

Stosujemy wzór eksponencjalny:

$$I(x) - 1 = e^{F(x)} - 1,$$

gdzie

$$F(x) = \sum_{n=1}^{\infty} nx^n/n! = \sum_{n=1}^{\infty} x^n/(n-1)! = x \sum_{n=1}^{\infty} x^{n-1}/(n-1)! = xe^x.$$

Stąd $I(x) = e^{xe^x}$.

Na zakończenie tego paragrafu omówimy pewien sposób obliczania wartości liczb Bella. Jak pamiętamy, eksponencjalną funkcją tworzącą dla liczb Bella jest

$\exp(e^x-1)$. Rozważmy operator liniowy $D-I$ i jego działanie na eksponencjalnych szeregach formalnych. Mamy

$$(D-I)\left(\sum_{n=0}^{\infty} a_n \frac{x^n}{n!}\right) = \sum_{n=0}^{\infty} a_{n+1} \frac{x^n}{n!} - \sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} (a_{n+1}-a_n) \frac{x^n}{n!}.$$

Innymi słowy, operator $D-I$ przyporządkowuje eksponencjalnemu szeregowi formalnemu reprezentującemu ciąg $\langle a_n\rangle_{n=0}^{\infty}$ szereg reprezentujący ciąg $\langle a_{n+1} - a_n\rangle_{n=0}^{\infty}$.

Niech $b = \exp(e^x-1)$. Mamy

$$(D-I)^n b = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j} D^j b.$$

Szereg $D^j b$ ma zaś postać $\sum_{m=0}^{\infty} B_{m+j} \frac{x^m}{m!}$. Zajmiemy się odnalezieniem współczynnika przy x w szeregu $(D-I)^n b$. Oznaczmy tę liczbę przez b_1^n. Mamy wtedy dla $n = N_0$

$$b_1^n = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j} B_{j+1}.$$

Zauważmy jednak, że $b_1^0 = 1$. Z równości

$$B_{n+1} = \sum_{j=0}^{n} \binom{n}{j} B_j$$

wynika (por. rozdział 2, wniosek 4.3(b)), że

$$B_n = \sum_{j=0}^{n} (-1)^{n-j}\binom{n}{j} B_{j+1}.$$

Stąd natychmiast otrzymujemy

$$b_1^n = B_n.$$

Ponieważ jednak dla każdego ciągu $\langle a_n\rangle_{n=0}^{\infty}$ mamy $a_{n+1} = a_n + (a_{n+1}-a_n)$, więc powyższa równość daje sposób znajdowania liczb Bella za pomocą prostej tablicy:

	1	2	3	4	5	6	7	8
b	1	2	5	15	52	203		
$(D-I)b$	1	3	10	37	151			
$(D-I)^2 b$	2	7	27	114				
$(D-I)^3 b$	5	20	87					
$(D-I)^4 b$	15	67						
$(D-I)^5 b$	52	255						
$(D-I)^6 b$	203							

Tablica ta powstaje jak następuje. Wiemy, że $B_1 = 1$, a zatem $b_1^1 = 1$. Równocześnie $b_1^1 = B_2 - B_1$. Stąd $B_2 = 2$, a zatem $b_1^2 = 2$. Wobec tego $b_2^2 = 2+1 = 3$ itd. Ogólnie, w tablicy naszej stoją liczby b_j^i, $i \in N_0$, $j \in N$. Przy tym kolejny wiersz jest ciągiem różnic elementów poprzedniego wiersza

$$b_i^{j+1} = b_{i+1}^j - b_i^j,$$

czyli

$$b_{i+1}^j = b_i^{j+1} + b_i^j.$$

To właśnie daje nam możliwość wypełnienia tablicy. Obok $b_1^4 = 15$ wpiszemy teraz $52+15 = 67$, obok 20 wpiszemy $67+20 = 87$, obok 27 wpiszemy $87+27 = 114$, obok 37 liczbę $114+37$, czyli 151, wreszcie obok 52 liczbę $151+52 = 203$, która jest liczbą B_6. Ta zaś z kolei równa jest b_1^6, co pozwala nam rozpocząć kolejną „przekątną" naszej tablicy.

§ 7. Iloczyny nieskończone, funkcje tworzące dla podziałów liczb

W algebrze szeregów formalnych wprowadzimy pewną topologię. Umożliwi nam to mówienie o zbieżności ciągów szeregów formalnych. Topologia ta jest istotnie słabsza od zwykłej topologii w pierścieniu funkcji analitycznych (np. zadanej przez normę „sup"). Rozważmy w C topologię dyskretną. W zbiorze C^{N_0} wszystkich ciągów mamy topologię produktową względem tej topologii. Topologia ta przenosi się na algebrę szeregów formalnych $C[\![x]\!]$. Zbadajmy, jak wygląda w tej topologii zbieżność. Niech zatem dany będzie ciąg $\langle f_n \rangle_{n=0}^{\infty}$ szeregów formalnych, $f_n = \sum_{m=0}^{\infty} a_{nm} x^m$. Ciąg $\langle f_n \rangle_{n=0}^{\infty}$ jest zbieżny do szeregu $f = \sum_{m=0}^{\infty} a_m x^m$ wtedy i tylko wtedy, gdy dla każdej współrzędnej m ciąg $\langle a_{nm} \rangle_{n=0}^{\infty}$ jest zbieżny w topologii dyskretnej do a_m. Innymi słowy, dla pewnego $n(m)$, wszystkie wyrazy a_{km}, dla $k > n(m)$, są równe a_m. Podobnie też wygląda zbieżność w algebrze szeregów formalnych większej liczby zmiennych. Fakt ten zostanie użyty poniżej. Istotne dla naszych celów jest to, że działania dodawania, mnożenia i odwracania, a także różniczkowania, są we wprowadzonej topologii ciągłe (Czytelnik obznajmiony z przestrzenią Baire'a nie będzie miał co do tego żadnych wątpliwości). Innymi słowy, zachodzi następujący lemat:

LEMAT 7.1. *Niech* $\lim_{n\to\infty}(\cdot)$ *będzie operacją granicy ciągu w sensie wprowadzonej powyżej „słabej" topologii. Niech* $\langle f_n \rangle_{n=0}^{\infty}$, $\langle g_n \rangle_{n=0}^{\infty}$ *będą dwoma ciągami szeregów formalnych, dla których istnieją granice* $\lim_{n\to\infty} f_n$ *i* $\lim_{n\to\infty} g_n$ *i niech* $a \in C$. *Wtedy*

(a) *istnieją granice* $\lim_{n\to\infty}(af_n)$, $\lim_{n\to\infty}(f_n+g_n)$, $\lim_{n\to\infty}(f_n \cdot g_n)$, $\lim_{n\to\infty} f_n'$ *oraz — jeśli szeregi* f_n *i* $\lim_{n\to\infty} f_n$ *są odwracalne —* $\lim_{n\to\infty}(f_n^{-1})$. *Ponadto*

(b) *zachodzą równości*

$$\lim_{n\to\infty}(af_n) = a\lim_{n\to\infty} f_n,$$

$$\lim_{n\to\infty}(f_n+g_n) = (\lim_{n\to\infty} f_n)+(\lim_{n\to\infty} g_n),$$

$$\lim_{n\to\infty}(f_n\cdot g_n) = (\lim_{n\to\infty} f_n)\cdot(\lim_{n\to\infty} g_n),$$

$$\lim_{n\to\infty} f_n' = (\lim_{n\to\infty} f_n)',$$

$$\lim_{n\to\infty}(f_n^{-1}) = (\lim_{n\to\infty} f_n)^{-1}.$$

Dowód. Pozostawiając dowód Czytelnikowi zauważmy jedynie, że zarówno w przypadku sumy, jak też iloczynu, różniczkowania i odwracania (por. dowód tw. 1.2), każdy z wyrazów wyniku zależy od skończonej liczby wyrazów szeregów wyjściowych. Stąd już łatwo wynika teza naszego lematu. □

Zauważmy, że szereg $\sum_{n=0}^{\infty} a_n x^n$ jest granicą ciągu swoich sum częściowych $\langle \sum_{j=0}^{n} a_j x^j \rangle_{n=0}^{\infty}$. Jednakże „słaba" topologia jest inna niż zwykła topologia, dziedziczona z klasy funkcji analitycznych. Na przykład, ciąg wielomianów $\langle (1/2^n)\cdot x \rangle_{n=0}^{\infty}$ nie jest zbieżny w słabej topologii.

Iloczynem nieskończonym $\prod_{j=0}^{\infty} f_j$ nazywamy szereg formalny $\lim_{n\to\infty}(\prod_{j=0}^{n} f_j)$, o ile taka granica istnieje.

Dla szeregu formalnego $f = \sum_{n=0}^{\infty} a_n x^n$ definiujemy $s(f)$ jako najmniejsze $n > 0$ takie, że $a_n \neq 0$. Następujące kryterium zbieżności iloczynów nieskończonych okazuje się użyteczne w dalszym ciągu rozważań.

LEMAT 7.2. *Niech* $\langle f_n \rangle_{n=0}^{\infty}$ *będzie ciągiem szeregów formalnych takim, że dla każdego* n, $f_n(0) = 1$. *Wtedy* $\prod_{n=0}^{\infty} f_n$ *jest zbieżny wtedy i tylko wtedy, gdy* $\liminf_{n\to\infty} s(f_n) = \infty$.

Dowód. (Przypomnijmy, że $\liminf_{n\to\infty} a_n$ to kres dolny granic podciągów nieskończonych ciągu $\langle a_n \rangle_{n=0}^{\infty}$.) Warunek $\liminf_{n\to\infty} s(f_n) = \infty$ oznacza, iż nie istnieje nieskończony podciąg ograniczony (a więc równoważnie, ponieważ wartości ciągu $s(f_n)$ są liczbami naturalnymi, że nie istnieje nieskończony podciąg stały). Zatem dla każdego $k \in N_0$ istnieje $m(k) \in N_0$ takie, że $s(f_r) > k$ dla $r > m(k)$. Stąd wnioskujemy, że poczynając od $m(k)$, wyrazy iloczynów częściowych mają te same wyrazy aż do k-tego. To zaś oznacza zbieżność naszego iloczynu. Załóżmy zatem, że $\liminf_{n\to\infty} s(f_n) < \infty$. Mamy, zgodnie z założeniem, $f_n(0) = 1$. Wobec powyższych

uwag istnieje ciąg $\langle n_k\rangle_{k=0}^{\infty}$ oraz $m\in N$ takie, że $s(f_{n_k})=m$, dla każdego k. Wybierzmy najmniejsze takie m. Zbadajmy jak wyglądają m-te wyrazy iloczynów $\prod_{j=0}^{n} f_j$. Skoro m jest najmniejszą niezerową liczbą naturalną, dla której istnieje podciąg wybrany jak wyżej, przeto od pewnego miejsca $s(f_r)\geqslant m$.

Niech

$$\prod_{j=0}^{r} f_j=\sum_{j=0}^{\infty} c_j x^j,\quad \prod_{j=0}^{r+1} f_j=\sum_{j=0}^{\infty} d_j x^j,\quad f_{r+1}=\sum_{j=0}^{\infty} e_j x^j.$$

Mamy $d_m=\sum_{i=0}^{m} c_i e_{m-i}$, możliwe są zatem następujące dwa przypadki:

(i) $d_m=c_m\cdot e_0$, jeśli $s(f_{r+1})>m$;

(ii) $d_m=c_m e_0+c_0 e_m$, jeśli $s(f_{r+1})=m$.

Wiemy przy tym, że dla nieskończenie wielu m zachodzi drugi przypadek. Co więcej, dla tych wartości $e_m\neq 0$, oraz, wobec $e_0=c_0=1$, mamy $d_m=c_m+e_m$, czyli $d_m\neq c_m$. Oznacza to, iż iloczyn nasz nie jest zbieżny. □

Wniosek 7.3. *Niech $\langle f_n\rangle_{n=0}^{\infty}$ będzie ciągiem szeregów formalnych, $f_n(0)=1$, a ciąg $\langle s(f_n)\rangle_{n=0}^{\infty}$ niech będzie ściśle rosnący. Wówczas iloczyn $\prod_{j=0}^{\infty} f_j$ jest zbieżny.*

Przypomnijmy, iż w rozdziale 1, § 11, wykazaliśmy używając formalizmu analitycznego (i pozostawiając kwestie zbieżności Czytelnikowi, zad. 71), że zachodzi następujące twierdzenie:

Twierdzenie 7.4 (Euler). *Funkcją tworzącą dla ciągu $\langle P(n)\rangle_{n=0}^{\infty}$, gdzie $P(n)$ jest liczbą podziałów liczby n, jest iloczyn nieskończony*

$$\prod_{j=0}^{\infty}(1-x^{j+1})^{-1}.$$

Zauważmy tylko, że $s\big((1-x^{j+1})^{-1}\big)=j+1$ i zatem do badania zbieżności iloczynu nieskończonego możemy użyć kryterium z wniosku 7.3.

Znajdziemy teraz funkcję tworzącą dla ciągu podwójnego $\langle P(n, m)\rangle_{n\in N, m\in N}$ ($P(n, m)$ jest liczbą podziałów liczby n na m składników).

Twierdzenie 7.5 (Euler). *Funkcją tworzącą dla ciągu podwójnego $\langle P(n, m)\rangle_{n\in N, m\in N}$ jest iloczyn nieskończony*

$$\prod_{j=0}^{\infty}(1-qx^{j+1})^{-1}$$

(tzn. $P(n, m)$ jest współczynnikiem przy $q^m x^n$).

Dowód. Łatwo widzieć, że nasz iloczyn jest zbieżny. Spełnia on bowiem kryterium analogiczne dla dowiedzionego we wniosku 7.3. Mamy

$$\prod_{j=0}^{\infty} (1-qx^{j+1})^{-1} = \prod_{j=0}^{\infty} \sum_{k=0}^{\infty} q^k x^{(j+1)k} = \sum_{k_1,\ldots,k_n \geq 0} q^{k_1+\ldots+k_n} x^{k_1+2k_2+\ldots+nk_n}.$$

Innymi słowy, współczynnik jednomianu $q^m x^n$ jest liczbą rozwiązań równania

$$k_1+2k_2+\ldots+nk_n = n,$$

dla których

$$k_1+\ldots+k_n = m. \quad \square$$

Zauważmy, że $\prod_{j=0}^{m-1} (1-x^{j+1})$ jest funkcją tworzącą dla ciągu $P_m(n)$, liczby podziałów liczby n, w których każdy składnik jest równy co najwyżej m. (Stosujemy po prostu rozumowanie z twierdzenia 7.5.) Wynika stąd następujący fakt.

Twierdzenie 7.6.

$$\prod_{j=0}^{\infty} (1-x^{j+1})^{-1} = \sum_{j=0}^{\infty} \frac{x^j}{(1-x)\ldots(1-x^j)}.$$

Dowód. Zgodnie z interpretacją kombinatoryczną współczynników lewej strony — $P(n)$ — i prawej strony — $P_1(n-1)+P_2(n-1)+\ldots$ — wystarczy wykazać równość

$$P(n) = P_1(n-1)+P_2(n-2)+\ldots$$

W tym celu zauważmy, że liczba $P_m(n)$ jest równa liczbie podziałów, z największym składnikiem równym m, liczby $n+m$. Aby się o tym przekonać, wystarczy do odpowiedniego diagramu Ferrersa (por. § 11, rozdz. 1) dodać kolumnę składającą się z m punktów.

Dowód twierdzenia jest teraz oczywisty: klasyfikujemy podziały liczby n według największego składnika. $\square$

Podobne rozważania dają dowód następującej tożsamości:

$$\prod_{j=0}^{\infty} (1-qx^{j+1})^{-1} = \sum_{j=0}^{\infty} \frac{q^j x^j}{(1-x)\ldots(1-x^j)}.$$

§ 8. Liczby Catalana

W paragrafie tym wskażemy na jeszcze jedno zastosowanie teorii funkcji tworzących. Zajmiemy się mianowicie następującym problemem:

Znaleźć liczbę c_n sposobów, którymi można rozmieścić nawiasy w iloczynie $x_1 \dots x_n$.

Przyjmujemy $c_0 = 0$. Mamy oczywiście $c_1 = 1$, $c_2 = 1$, $c_3 = 2$, przy czym w tym ostatnim przypadku mamy następujące rozmieszczenia nawiasów: $(x_1 x_2) x_3$ i $x_1 (x_2 x_3)$. Zauważmy, że dla $n > 1$ każde wyrażenie f zdefiniowane przez rozmieszczenie nawiasów w iloczynie długości n ma postać $f = gh$ dla pewnych wyrażeń g, h takich, że g zawiera zmienne $x_1, \dots, x_k$, zaś h zmienne $x_{k+1}, \dots, x_n$, przy czym $0 < k < n$. Wyrażenia g, h — a więc i liczba k — są przy tym jednoznacznie wyznaczone przez f. Każda wartość k odpowiada oczywiście $c_k c_{n-k}$ różnym wyrażeniom f. Stąd dla $n > 1$ mamy

$$c_n = c_1 c_{n-1} + c_2 c_{n-2} + \dots + c_{n-1} c_1 = c_0 c_n + c_1 c_{n-1} + \dots + c_n c_0$$

(korzystamy z faktu, iż $c_0 = 0$). Rozpoznajemy tu wzór na współczynniki iloczynu Cauchy'ego szeregów formalnych. Dokładniej, łatwo widzieć, że szereg formalny $f_c = \sum_{n=0}^{\infty} c_n x^n$ spełnia równanie

$$f_c^2 - f_c + x = 0. \tag{8.1}$$

Można łatwo wykazać, że rozwiązania tego równania mają, tak jak w przypadku równań kwadratowych w dziedzinie liczb zespolonych, postać $f_c = \frac{1}{2}(1+g)$, gdzie g jest szeregiem formalnym (jednym z dwu możliwych) takim, że $g^2 = 1-4x$. Taki szereg g łatwo znajdujemy rozwijając w szereg Maclaurina funkcję $g(x) = \sqrt{1-4x}$. Korzystając ze wzoru $a_n = \frac{1}{n!}[D^n g]_{x=0}$ mamy

$$a_n = (-4)^n \frac{\frac{1}{2}(\frac{1}{2}-1)(\frac{1}{2}-2)\dots(\frac{1}{2}-(n-1))}{n!} =$$

$$= (-1) \cdot \frac{4^n \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{3}{2} \dots \frac{1}{2}(2n-3)}{n!} = (-1) \cdot \frac{2^n 1 \cdot 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-3)}{n!} =$$

$$= (-1) \cdot \frac{2^n 1 \cdot 1 \cdot 3 \cdot 5 \dots (2n-3) \cdot (n-1)!}{n!(n-1)!} =$$

$$= (-1) \frac{2}{n} \frac{(2n-2)!}{(n-1)!(n-1)!} = (-1) \cdot \frac{2}{n} \binom{2n-2}{n-1}.$$

Wynika stąd, że $f_c = \frac{1-\sqrt{1-4x}}{2}$, gdyż musi być $f_c(0) = 0$. Zatem $c_n = -a_n/2$ dla $n \geqslant 1$, i ostatecznie

$$c_n = \frac{1}{n} \binom{2n-2}{n-1}.$$

Liczby c_n nazywamy *liczbami Catalana*.

Liczby Catalana pojawiają się też przy zliczaniu tzw. drzew binarnych. Przez *drzewo binarne o n wierzchołkach* rozumiemy *drzewo puste* $T = \emptyset$, jeśli $n = 0$, lub trójkę $T = \langle L, r, P\rangle$, gdzie r jest wierzchołkiem zwanym *korzeniem drzewa*, L (*lewe poddrzewo*) jest drzewem binarnym o l wierzchołkach, P (*prawe poddrzewo*) jest drzewem binarnym o p wierzchołkach i $l+p+1 = n$. Mówimy, że drzewa binarne T_1 i T_2 są *izomorficzne*, co oznaczamy $T_1 \approx T_2$, jeśli $T_1 = T_2 = \emptyset$ lub $T_1 = \langle L_1, r_1, P_1\rangle$, $T_2 = \langle L_2, r_2, P_2\rangle$, gdzie $L_1 \approx L_2$ i $P_1 \approx P_2$. Oznaczmy przez d_n



Rys. 18. Drzewa binarne o n wierzchołkach, $n = 0, 1, 2, 3$.

liczbę nieizomorficznych drzew binarnych o n wierzchołkach (por. rys. 18). Z podanych definicji rekurencyjnych wynika, że $d_0 = 1$ oraz jeśli $0 \leqslant k \leqslant n$, to istnieje dokładnie $d_k d_{n-k-1}$ nieizomorficznych drzew binarnych $\langle L, r, P\rangle$ o n wierzchołkach, takich, że L jest drzewem binarnym o k wierzchołkach. Liczba k może przyjmować każdą z wartości między 0 a $n-1$, zatem dla $n > 0$

$$d_n = d_0 d_{n-1} + d_1 d_{n-2} + \ldots + d_{n-1} d_0.$$

Dla funkcji tworzącej $f_d = \sum_{n=0}^{\infty} d_n x^n$ otrzymujemy stąd równanie

$$xf_d^2 - f_d + 1 = 0.$$

Wystarczy teraz podstawić $f_d = g/x$ aby otrzymać równanie

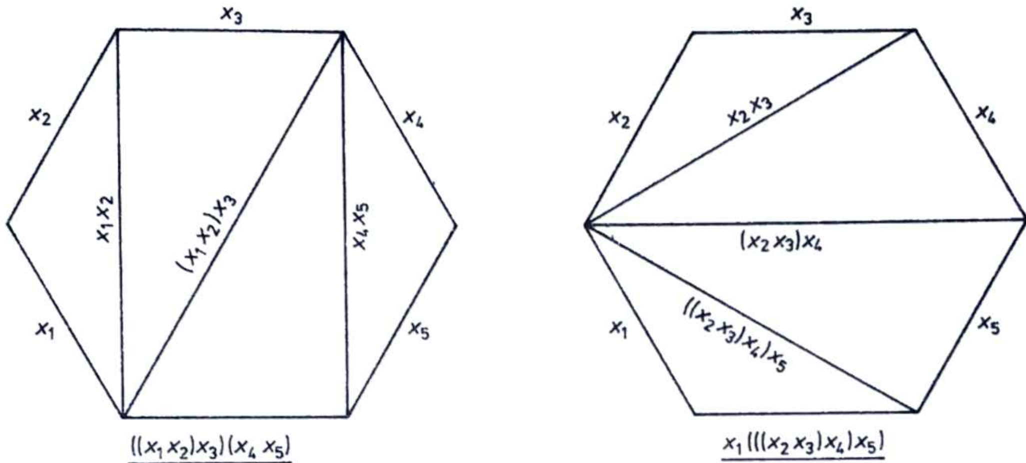
$$x\frac{g^2}{x^2} - \frac{g}{x} + 1 = 0,$$

czyli

$$g^2 - g + x = 0.$$

Porównując to równanie z (8.1) stwierdzamy, że g jest funkcją tworzącą dla liczb Catalana. A zatem $d_n = c_{n+1}$, $n \in N_0$.

Innym przykładem zadania, redukującego się do szukania liczb Catalana, jest problem liczby t_n triangulacji wielokąta wypukłego o n bokach za pomocą rodziny parami nie przecinających się przekątnych (p. rys. 19).



Rys. 19. Dwie różne triangulacje sześciokąta wypukłego wraz z odpowiadającymi im wyrażeniami

Dla rozwiązania tego zadania przyporządkujmy kolejnym $n-1$ bokom naszego wielokąta zmienne $x_1, \ldots, x_{n-1}$, a następnie kolejno (zachowując porządek zmiennych) wyrażenia kolejnym odcinkom na naszym rysunku, stosując następującą regułę: Jeśli α i β są wyrażeniami przypisanymi krawędziom, a kolejna krawędź tworzy trójkąt wraz z tymi krawędziami, to przypisujemy jej wyrażenie $\alpha\beta$. Procedura ta jest pokazana na rys. 19.

Tak opisane przyporządkowanie jest różnowartościowe i „na". W ten sposób bez trudu stwierdzamy, że liczba t_n triangulacji n-kąta jest równa c_{n-1} $(n \geqslant 3)$.

Zadania

1. Sprawdzić, że mnożenie szeregów formalnych jest działaniem przemiennym.

2. Udowodnić lemat 1.1.

3. Wskazać indukcyjną procedurę znajdowania odwrotności szeregu formalnego $\sum_{n=0}^{\infty} a_n x^n$, gdzie $a_0 \neq 0$.

4. *Formalnym szeregiem Laurenta* nazywamy wyrażenie $\sum_{n=-\infty}^{\infty} a_n x^n$, gdzie $a_n = 0$ dla prawie wszystkich ujemnych n. Korzystając z tożsamości $\sum_{j=k}^{\infty} a_j x^j = x^k \sum_{j=0}^{\infty} a_{j+k} x^j$ wykazać, że szeregi formalne Laurenta tworzą ciało izomorficzne z ciałem ułamków pierścienia szeregów formalnych.

5. Niech $v, w \in C[\![x]\!]$. Wykazać, że

$$D(v \cdot w) = w \cdot Dv + v \cdot Dw.$$

Znaleźć uogólnienie powyższego wzoru dla wielokrotnego różniczkowania (wzór Leibniza).

6. Niech $v, w \in C[\![x]\!]$, przy tym niech w będzie szeregiem odwracalnym. Wykazać, że

$$D(v\cdot w^{-1}) = [D(v)\cdot w - v\cdot D(w)]\cdot (w^{-1})^2.$$

7. Niech $v \in C[\![x]\!]$, $n \in N$. Wykazać, że

$$D(v^n) = n\cdot v^{n-1}\cdot Dv.$$

8. Niech $v, w \in C[\![x]\!]$ i niech rodzina w^i: współczynnik przy x^i w v jest różny od zera będzie sumowalna. Wykazać, że

$$D(v(w)) = (Dv)(w)\cdot Dw.$$

Wskazówka: Wykazać, że szereg $v(w)$ można zróżniczkować „wyraz po wyrazie" względem w i skorzystać z wyniku zadania 7.

9. Wykazać, że jeżeli $w = \sum_{n=0}^{\infty} w_n x^n$, to $w_n = \frac{1}{n!}\cdot (D^n w)(0)$.

10. Definiujemy szeregi formalne $(1-x)^a$, gdzie $a \in C$ i $\ln(1-x)$ jako odpowiednio $\sum_{n=0}^{\infty} [a]_n(-x)^n/n!$ i $\sum_{n=1}^{\infty} -x^n/n$. Wykazać, iż szeregi

$$a\ln(1-x) \quad \text{oraz} \quad \ln(1-x)^a$$

są równe.

11. Niech $f \in \mathscr{A}(P)$ będzie funkcją odwracalną (tj. dla każdego x, $f(x, x) \neq 0$). Niech h będzie elementem algebry incydencji określonym wzorem:

$$h(x, x) = f(x, x),$$

$$h(x, y) = 0, \quad \text{jeśli } x \neq y.$$

Niech wreszcie $g = (h-f) * h^{-1}$. Określamy $k \in \mathscr{A}(P)$ jak następuje: Jeśli maksymalną długością łańcucha w odcinku $[x, y]$ jest $n \in N_0$, to

$$k(x, y) = \delta(x, y) + g(x, y) + \ldots + g^n(x, y).$$

(a) Wykazać, że $h^{-1} * k$ jest funkcją odwrotną do f.

(b) Wykorzystać udowodniony w punkcie (a) fakt dla dowodu, iż odwrotność odwracalnej funkcji niezmienniczej ze względu na przesunięcie ma także tę własność.

12. Niech $P_6 = \langle Z, \leqslant \rangle$. Wykazać, że P_6 ma własność dwumianową. Znaleźć zredukowaną algebrę incydencji $\mathscr{R}(P_6)$.

13. Niech $P_7 = \langle U, \leqslant \rangle$, gdzie U składa się z „sześcianów" $A\times B\times C \subseteq_{\text{fin}} N^3$ takich, że $|A| = |B| = |C|$. Wykazać, że P_7 ma własność dwumianową. Znaleźć $\mathscr{R}(P_7)$ i izomorfizm tej algebry z odpowiednim pierścieniem szeregów formalnych.

14. (Kreid). Niech $\langle v_n(x)\rangle_{n=0}^{\infty}$ będzie dwumianowym ciągiem wielomianów i niech $V_n(x) = \sum_{k=0}^{n} V(n, k)x^k$. Wówczas $V(n, 0) = 0$ oraz istnieje a takie, że dla wszystkich n, $V(n, n) = a^n$.

15. (Kreid). Jeśli α jest podziałem liczby n, $n = k_1 i_1 + \ldots + k_r i_r$, to przez $B(\alpha)$ rozumiemy liczbę $n!/(i_1!\cdot\ldots\cdot i_r!\cdot(k_1!)^{i_1}\cdot\ldots\cdot(k_r!)^{i_r})$. Wreszcie, jeśli $a = \langle a_n\rangle_{n\in N_0}$, zaś $\alpha = \langle k_1 \ldots k_m\rangle$ jest podziałem liczby n, to a_α definiujemy jako $a_{k_1}\cdot\ldots\cdot a_{k_m}$, zaś $|\alpha| = m$.

Przy powyższych definicjach prawdziwe są następujące fakty:

(a) Jeśli dany jest ciąg $\langle a_n \rangle_{n\in N}$, $a_1 \neq 0$, to ciąg wielomianów

$$V_n(x) = \sum B(\alpha)\cdot a_\alpha x^{|\alpha|},$$

gdzie α przebiega wszystkie podziały liczby n, jest dwumianowy.

(b) Każdy ciąg dwumianowy jest powyższej postaci.

16. Wykazać, że zbiór operatorów niezmienniczych ze względu na przesunięcia tworzy podalgebrę algebry operatorów liniowych w przestrzeni wielomianów.

17. Znaleźć delta operator, którego bazą jest ciąg tzw. *wielomianów eksponencjalnych* $\langle \Phi_n(x)\rangle_{n=0}^{\infty}$, gdzie

$$\Phi_n(x) = \sum_{k=0}^{n} S(n, k)\, x^k.$$

18. Korzystając z wyniku zadania 17 wykazać, że ciąg wielomianów eksponencjalnych jest typu dwumianowego.

19. Korzystając z wyniku zadania 15 wykazać, że ciąg wielomianów eksponencjalnych jest typu dwumianowego.

20. Znaleźć bazy dla operatora Bernoulliego i średniej Eulera.

21. Znaleźć rozwinięcia wielomianu x^n odpowiednio w bazach $\langle [x]^n\rangle_{n=0}^{\infty}$ i $\langle [x]_n\rangle_{n=0}^{\infty}$.

22. Korzystając z równości $E-E^{-1/2} = \Delta(I+\Delta)^{-1/2} = \nabla(I-\nabla)^{-1/2}$ wykazać, że dla $n>0$,

$$x[x+n/2-1]_{n-1} = \sum_{k=0}^{n} \binom{n-1}{k}[n/2]_k [x]_{n-k} = \sum_{k=0}^{n} \binom{n-1}{k}[-n/2]^k [x]^{n-k}.$$

23. Niech $f\colon C \to C$ będzie dowolną funkcją. *Tablicą różnicową* funkcji f nazywamy tablicę trójkątną, która w zerowym wierszu zawiera ciąg wartości $\langle f(n)\rangle_{n=0}^{\infty}$, a n-ty wyraz kolejnego wiersza jest różnicą $(n+1)$-ego i n-tego wyrazu wiersza poprzedniego. Dopisując wiersz do tablicy przesuwamy go o pół kolumny w prawo tak, że każdy wyraz jest różnicą wyrazów stojących nad nim. Na przykład, dla funkcji $f(x) = x^3$ mamy

$f(x)$	0	1	8	27	64	125	216	...
$\Delta f(x)$		1	7	19	37	61	91	......
$\Delta^2 f(x)$			6	12	18	24	30	....
$\Delta^3 f(x)$				6	6	6	6	....
$\Delta^4 f(x)$					0	0	0	....
						0	0	....
							0	....

Wykazać, iż przyporządkowanie funkcji jej tablicy różnicowej jest odwzorowaniem liniowym.

24. Wykazać, że jeśli $k\in N_0$, zaś $f(x)$ jest wielomianem stopnia nie większego niż $k-1$, to k-ty wiersz tablicy różnicowej jest stale równy zeru.

25. Wykazać następujący fakt odwrotny do wyniku zadania 24: Jeśli k-ty wiersz tablicy różnicowej jest złożony z samych zer, to istnieje wielomian $w(x)$ stopnia mniejszego niż k, którego tablica nasza jest tablicą różnicową.

26. Wykazać, że ciąg $\langle \Delta^k f(0)\rangle_{k=0}^{\infty}$ zwany *lewą krawędzią* tablicy wyznacza całą tablicę.

27. Wykazać, że jeśli $\Delta^k f(0) = 1$, oraz $\Delta^n f(0) = 0$ dla $n \neq k$, to rozważana tablica jest tablicą różnicową dla wielomianu

$$\binom{x}{k} = [x]_k/k!.$$

28. Korzystając z zadań 23 i 27 wywnioskować, że jeśli lewa krawędź tablicy jest ciągiem $\langle c_k \rangle_{k=0}^{\infty}$, przy tym, dla $k > n$, $c_k = 0$, to tablica odpowiada wielomianowi

$$w(x) = \sum_k c_k \binom{x}{k}.$$

29. Korzystając z tożsamości

$$\binom{0}{k} + \binom{1}{k} + \ldots + \binom{m}{k} = \binom{m+1}{k+1}$$

(por. rozdz. 1, wzór (5.9)) udowodnić, iż dla dowolnego wielomianu $w(x)$ mamy

$$\sum_{k=0}^{n} w(k) = c_0 \binom{n+1}{1} + c_1 \binom{n+1}{2} + \ldots + c_n \binom{n+1}{n+1}$$

gdzie $\langle c_j \rangle_{j=0}^{\infty}$ jest lewą krawędzią tablicy różnicowej wielomianu $w(x)$.

30. Korzystając z wyniku zadania 29 znaleźć wzory na sumy czwartych i piątych potęg liczb naturalnych.

31. Uogólnić rozwijanie wielomianów w bazie $\langle [x]_n \rangle_{n=0}^{\infty}$ za pomocą tablic różnicowych (zad. 28) na szeregi formalne.

32. Zbudować analogiczną „technikę tablic różnicowych” dla operatora ∇.

33. Znaleźć funkcję tworzącą $f_{\boldsymbol{a}}$ dla następujących ciągów $\boldsymbol{a}$:

(a) $a_n = \binom{n+k}{n}$, gdzie k jest ustaloną liczbą naturalną i $k \geqslant 1$;

(b) $a_n = n^4$;

(c) $a_n = n^5$;

(d) $a_n = \begin{cases} 0 & \text{dla } n = 0, \\ 1/n & \text{dla } n > 0; \end{cases}$

(e) $a_n = \begin{cases} 0 & \text{dla } n \text{ parzystego lub } n = 3, \\ 1/n & \text{dla } n \text{ nieparzystego, różnego od } 3; \end{cases}$

(f) $a_n = \begin{cases} 0 & \text{dla } n \text{ nieparzystego lub } n = 0, \\ 1/n & \text{dla } n \text{ parzystego i większego od zera}; \end{cases}$

(g) $a_n = \begin{cases} 0 & \text{dla } n \text{ parzystego}, \\ 1/n! & \text{dla } n \text{ nieparzystego}. \end{cases}$

34. Znaleźć wzór rekurencyjny (względem k) dla funkcji tworzącej ciągu $\langle a_n^k \rangle_{n=1}^{\infty}$, gdzie $a_n^k = n^k$.

Wskazówka: $f_{a^1} = \dfrac{x}{(1-x)^2}$, $f_{a^2} = \dfrac{x(1+x)}{(1-x)^3}$.

35. Znaleźć eksponencjalną funkcję tworzącą dla następujących ciągów $\boldsymbol{a}$:

(a) $a_n = n$;

(b) $a_n = n+1$;

(c) $a_n = \begin{cases} 0 & \text{dla } n \text{ parzystego}, \\ 1 & \text{dla } n \text{ nieparzystego}. \end{cases}$

36. Jakie związki zachodzą pomiędzy eksponencjalnymi funkcjami tworzącymi ciągów a i b i c, jeśli

(a) $a_n = \sum_{k=0}^{n} b_k c_{n-k}$;

(b) $a_n = \sum_{k=0}^{n} b_k b_{n-k}$;

(c) $a_n = \sum_{k=0}^{n} b_k$;

(d) $a_n = b_{n+1} - b_n$.

37. Znaleźć rozwiązanie uogólnionego równania Fibonacciego: $a_0 = a$, $a_1 = b$, $a_{n+2} = a_{n+1} + a_n$, gdzie a, b są ustalonymi liczbami zespolonymi.

38. Wykazać, że rozwiązania równania różnicowego

$$c_1 a_n + \ldots + c_k a_{n+k} = 0$$

tworzą podprzestrzeń liniową przestrzeni ciągów C^N. Jaki jest wymiar takiej podprzestrzeni?

39. Wykazać, że ciągi $\langle a_n \rangle_{n\in N}$, $a_n = \left(\frac{1+\sqrt{5}}{2}\right)^{n+1}$, i $\langle b_n \rangle_{n\in N}$, $b_n = \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}$, tworzą bazę dla podprzestrzeni rozwiązań równania Fibonacciego: $a_{n+2} - a_{n+1} - a_n = 0$. Korzystając z powyższego rozwiązać równanie Fibonacciego nie wykorzystując metody funkcji tworzących.

40. Znaleźć liczbę $k_{2,3}$ funkcji $f\colon X \to X$, gdzie $|X| = n$, spełniających warunek $f^2(x) = f^3(x)$.

Wskazówka: Zastosować wzór eksponencjalny.

41 (Cayley). Zastosować wzór eksponencjalny dla znalezienia liczności zbioru drzew o n-elementowym zbiorze krawędzi i wyróżnionym wierzchołku.

42. Wykazać, że

$$\prod_{j=0}^{\infty} (1 - x^{j+1}) = \sum_{j=0}^{\infty} \varepsilon_j x^j,$$

gdzie $\varepsilon_j = 0$, jeśli j nie jest liczbą postaci $k(3\pm 1)/2$, a $\varepsilon_j = (-1)^k$, jeśli j jest liczbą postaci $k(3k\pm 1)/2$.

43. Korzystając z następującej formy wyniku zadania 42:

$$\prod_{j=0}^{\infty} (1 - x^{j+1}) = \sum_{k=1}^{\infty} (-1)^k (x^{k(3k+1)/2} + x^{k(3k-1)/2})$$

oraz faktu, iż $\sum_{j=0}^{\infty} P(j) x^j$ jest odwrotnością iloczynu $\prod_{j=0}^{\infty} (1 - x^{j+1})$ wykazać „twierdzenie pentagonalne Eulera", to znaczy równość

$$P(n) = \sum_{k=1}^{\infty} (-1)^{k-1} \left(P\left(n - \frac{k(3k-1)}{2}\right) + P\left(n - \frac{k(3k+1)}{2}\right) \right).$$

44. Wykazać, iż funkcją tworzącą dla podziałów liczb na części nieparzyste jest $\prod_{j=0}^{\infty} (1 - x^{2j+1})$.

45 (Chung, Feller). Rozważmy zbiór punktów kratowych na płaszczyźnie. *Drogą* z punktu $\langle 0, 0 \rangle$ do punktu $\langle n, n \rangle$ nazywamy ciąg odcinków postaci $[\langle i, j \rangle, \langle i+1, j \rangle]$ lub $[\langle i, j \rangle, \langle i, j+1 \rangle]$, taki, że pierwszy z tych odcinków zaczyna się w punkcie $\langle 0, 0 \rangle$, ostatni kończy się w punkcie $\langle n, n \rangle$, początek zaś kolejnego odcinka jest końcem poprzedniego.

(a) Wykazać, że istnieje dokładnie $d_n = \binom{2^n}{n}$ dróg z punktu $\langle 0, 0 \rangle$ do punktu $\langle n, n \rangle$.

(b) Wykazać, że $1/\sqrt{1-4x}$ jest funkcją tworzącą ciągu $\langle d_n \rangle_{n\in N}$.

(c) Wykazać, że zbiór dróg przebiegających poniżej przekątnej (to znaczy rozłącznych z górną półpłaszczyzną otwartą) liczy c_n elementów, gdzie c_n jest liczbą Catalana.

ROZDZIAŁ 4

ZAGADNIENIA MINIMAKSOWE I SYSTEMY REPREZENTANTÓW

Mianem twierdzeń minimaksowych określa się zwykle twierdzenia, które orzekają, iż minimalna wartość pewnej wielkości jest równa maksymalnej wartości innej wielkości. Najczęściej obie te wielkości mogą przyjmować wartości ze zbioru liczb całkowitych (lub rzeczywistych). Mogą być na przykład licznościami pewnych zbiorów. Najważniejszym chyba z twierdzeń minimaksowych, które podamy w tym rozdziale, jest twierdzenie Dilwortha. Mówi ono, że w dowolnym skończonym zbiorze częściowo uporządkowanym $\langle P, \leqslant \rangle$ maksymalna liczność antyłańcucha jest równa minimalnej liczbie łańcuchów, które pokrywają P. Aby prosto i przejrzyście sformułować to twierdzenie użyliśmy tu wyrażenia „maksymalna liczność antyłańcucha" do określenia liczby

$$M = \max\{|A|: A \text{ jest antyłańcuchem w } \langle P, \leqslant \rangle\}$$

(zauważmy przy okazji, że może być wiele antyłańcuchów o liczności M; każdy z nich jest maksymalny, lecz mogą też istnieć antyłańcuchy maksymalne o liczności mniejszej niż M). Podobnie przez „minimalną liczbę łańcuchów, które pokrywają P" rozumiemy liczbę

$$m = \min\{k: \text{istnieją łańcuchy } L_1, \ldots, L_k \text{ takie, że } L_1 \cup \ldots \cup L_k = P\}.$$

Sformułowań tego typu będziemy używali również przy omawianiu innych zagadnień minimaksowych.

Innym fundamentalnym twierdzeniem tego rozdziału jest klasyczne twierdzenie P. Halla o systemach reprezentantów podające warunek konieczny i dostateczny na to, by z danych zbiorów $A_1, \ldots, A_n$ (niekoniecznie rozłącznych) można było wybrać elementy $x_1 \in A_1, \ldots, x_n \in A_n$ tak, aby były one parami różne. Choć samo twierdzenie Halla nie ma postaci minimaksowej, wiele ściśle z nim związanych twierdzeń (np. twierdzenia Halla–Ore będące jego uogólnieniem, czy też twierdzenie węgierskie) orzeka równość pewnego maksimum i pewnego minimum, lub też może być łatwo przeformułowanych do takiej postaci. Okazuje się również, że większość twierdzeń o systemach reprezentantów można otrzymać jako prosty wniosek z twierdzenia Dilwortha.

Będziemy zajmowali się również w tym rozdziale, między innymi, pewnymi – związanymi z twierdzeniem Dilwortha – ekstremalnymi własnościami rodzin zbiorów, prostokątami i kwadratami łacińskimi oraz macierzami bistochastycznymi.

§ 1. Twierdzenie Dilwortha

Twierdzenie to dotyczy struktury zbiorów częściowo uporządkowanych, będziemy używali więc pojęć dotyczących porządku częściowego, takich jak element maksymalny, łańcuch, antyłańcuch itp. Wszystkie te pojęcia zdefiniowano w rozdziale 1 (§ 2).

TWIERDZENIE 1.1 (Dilworth [1]). *W dowolnym skończonym zbiorze częściowo uporządkowanym $\langle P, \leqslant \rangle$ maksymalna liczność antyłańcucha jest równa minimalnej liczbie łańcuchów, które pokrywają P.*

Dowód (Tverberg [1]). Stosujemy indukcję względem liczności zbioru P. Dla $|P| \leqslant 1$ twierdzenie jest oczywiście prawdziwe. Niech zatem $|P| > 1$, niech m będzie maksymalną licznością antyłańcucha w P i niech L będzie dowolnym łańcuchem maksymalnym w P. Jeśli każdy antyłańcuch w $P \setminus L$ ma co najwyżej $m-1$ elementów, to P jest sumą łańcucha L i $m-1$ łańcuchów, na które – na mocy założenia indukcyjnego – można rozłożyć $P \setminus L$. Załóżmy więc, że w $P \setminus L$ istnieje antyłańcuch m-elementowy $A = \{a_1, \ldots, a_m\}$. Utwórzmy zbiory

$$G = \{x \in P\colon \text{ istnieje } a \in A \text{ takie, że } x \geqslant a\},$$

$$D = \{x \in P\colon \text{ istnieje } a \in A \text{ takie, że } x \leqslant a\}.$$

Niech c będzie elementem minimalnym łańcucha L. Mamy $c \notin G$, w przeciwnym bowiem razie łańcuch L można by powiększyć o pewien element $a \in A$, $a < c$. Podobnie D nie zawiera elementu maksymalnego łańcucha L. Zatem $|G| < |P|$, $|D| < |P|$ i na mocy założenia indukcyjnego istnieją rozkłady na łańcuchy

$$G = G_1 \cup \ldots \cup G_m, \qquad D = D_1 \cup \ldots \cup D_m.$$

Bez zmniejszenia ogólności możemy zakładać, że $a_i \in G_i$, $a_i \in D_i$ dla $1 \leqslant i \leqslant m$. Antyłańcuch A jest m-elementowy, a więc maksymalny w P. Zatem $P = G \cup D$ (gdyż w przeciwnym razie $A \cup \{x\}$, $x \in P \setminus (G \cup D)$ byłby antyłańcuchem $(m+1)$-elementowym), i

$$P = (D_1 \cup G_1) \cup \ldots \cup (D_m \cup G_m)$$

jest rozkładem zbioru P na m łańcuchów. Oczywiście m jest minimalną liczbą łańcuchów, którymi można pokryć P, gdyż każdy łańcuch może zawierać co najwyżej jeden element antyłańcucha. □

Interesujący jest fakt, że twierdzenie Dilwortha prawdziwe jest również, gdy w jego sformułowaniu zamienimy miejscami słowa „łańcuch" i „antyłańcuch".

Twierdzenie 1.2 (dualne twierdzenie Dilwortha). *W dowolnym skończonym zbiorze częściowo uporządkowanym* $\langle P, \leqslant\rangle$ *maksymalna liczność łańcucha jest równa minimalnej liczbie antyłańcuchów, które pokrywają* P.

Dowód. Niech m będzie maksymalną licznością łańcucha w P. Każdy antyłańcuch może zawierać najwyżej jeden element łańcucha, nie może zatem istnieć rozkład zbioru P na mniej niż m antyłańcuchów. By dowieść twierdzenia, wystarczy zatem pokazać rozkład na m antyłańcuchów. Niech A_k oznacza zbiór elementów rangi k w $\langle P, \leqslant\rangle$. Oczywiście dla dowolnego k zbiór A_k jest antyłańcuchem i $P = A_0 \cup \ldots \cup A_{m-1}$. □

Jest jasne, że w obu powyższych twierdzeniach możemy ograniczyć się do rozkładów na łańcuchy (antyłańcuchy) rozłączne, gdyż dowolny rozkład $P = P_1 \cup \ldots \cup P_m$ możemy zastąpić przez rozkład $P = P'_1 \cup \ldots \cup P'_m$, gdzie $P'_i = P_i \setminus \bigcup_{j<i} P_j$ (nie żądamy by łańcuchy i antyłańcuchy były niepuste).

Podamy teraz szereg zastosowań twierdzenia Dilwortha.

Lemat 1.3. *Każdy zbiór częściowo uporządkowany o* $rs+1$ *elementach zawiera łańcuch o liczności* $r+1$ *lub antyłańcuch o liczności* $s+1$.

Dowód. Jeśli w zbiorze P nie istnieje łańcuch o liczności $r+1$, to, na mocy twierdzenia 1.2, zbiór P można przedstawić w postaci sumy r antyłańcuchów, $P = A_1 \cup \ldots \cup A_r$. Skoro $rs+1 \leqslant |A_1| + \ldots + |A_r|$, to dla pewnego i musi być $|A_i| \geqslant s+1$. □

Zauważmy, że powyższy lemat można wyprowadzić w analogiczny sposób z twierdzenia Dilwortha.

Twierdzenie 1.4. *Każdy ciąg* $n \geqslant rs+1$ *liczb rzeczywistych zawiera podciąg niemalejący o długości* $r+1$ *lub podciąg malejący o długości* $s+1$.

Dowód. Niech $a_1, a_2, \ldots, a_n$ będzie naszym ciągiem. Tworzymy zbiór $P = \{\langle k, a_k\rangle : 1 \leqslant k \leqslant n\}$ i wprowadzamy w nim porządek częściowy następująco:

$$\langle k, a_k\rangle \leqslant \langle j, a_j\rangle \Leftrightarrow k \leqslant j \wedge a_k \leqslant a_j.$$

Na mocy lematu 1.3 zbiór P zawiera łańcuch $(r+1)$-elementowy

$$\{\langle k_1, a_{k_1}\rangle, \langle k_2, a_{k_2}\rangle, \ldots, \langle k_{r+1}, a_{k_{r+1}}\rangle\}$$

$(k_1 < k_2 < \ldots < k_{r+1})$ lub antyłańcuch $(s+1)$-elementowy

$$\{\langle j_1, a_{j_1}\rangle, \langle j_2, a_{j_2}\rangle, \ldots, \langle j_{s+1}, a_{j_{s+1}}\rangle\}$$

$(j_1 < j_2 < \ldots < j_{s+1})$. W pierwszym przypadku $a_{k_1} \leqslant a_{k_2} \leqslant \ldots \leqslant a_{k_{r+1}}$, w drugim zaś $a_{j_1} > a_{j_2} > \ldots > a_{j_{s+1}}$. □

Jako szczególny przypadek otrzymujemy

Twierdzenie 1.5 (Erdös i Szekeres [1]). *Każdy ciąg* r^2+1 *liczb rzeczywistych zawiera podciąg monotoniczny długości* $r+1$. □

Jest jasne, że twierdzenia 1.4 i 1.5 są prawdziwe dla ciągów o elementach z dowolnego zbioru liniowo uporządkowanego.

Następne twierdzenie, zwane „twierdzeniem węgierskim", sformułujemy w języku macierzy zero-jedynkowych (tzn. o elementach 0 i 1). Przez *linię* będziemy rozumieli dowolny wiersz lub kolumnę macierzy, a przez *rozproszony zbiór jedynek* dowolny zbiór jedynek (ściślej mówiąc wystąpień jedynek w macierzy), z których żadne dwie nie leżą na tej samej linii.

TWIERDZENIE 1.6 (König [1], Egerváry [1]). *W każdej macierzy zero-jedynkowej minimalna liczba linii, którymi można pokryć wszystkie jedynki, jest równa maksymalnej liczności rozproszonego zbioru jedynek.*

Dowód. Niech nasza macierz $[a_{ij}]$ ma m wierszy i n kolumn. Utwórzmy pomocnicze zbiory $X = \{x_1, \ldots, x_m\}$, $Y = \{y_1, \ldots, y_n\}$, $P = X \cup Y$, których elementy identyfikujemy odpowiednio z wierszami, kolumnami i liniami macierzy $[a_{ij}]$ (zakładamy $X \cap Y \neq \emptyset$). W zbiorze P określamy porządek częściowy $\leqslant$ tak, by $a \leqslant b$ wtedy i tylko wtedy, gdy $a = x_i$, $b = y_j$ i $a_{ij} = 1$ dla pewnych i, j $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$.

Wprowadźmy oznaczenia:

l = minimalna liczba linii pokrywających wszystkie jedynki,
q = maksymalna liczność antyłańcucha w $\langle P, \leqslant \rangle$,
k = maksymalna liczność rozproszonego zbioru jedynek,
r = minimalna liczba łańcuchów, na które można rozłożyć P.

Mamy

$$l = m+n-q, \tag{1.1}$$

gdyż zbiór $A \subseteq P$ jest antyłańcuchem wtedy i tylko wtedy, gdy $P \setminus A$ jest zbiorem linii pokrywających wszystkie jedynki (przez każdą jedynkę przechodzą dwie linie, z których antyłańcuch zawiera najwyżej jedną). Każdy niepusty łańcuch w $\langle P, \leqslant \rangle$ składa się z jednego lub dwu elementów, przy czym każdemu zbiorowi złożonemu z rozłącznych łańcuchów dwuelementowych odpowiada rozproszony zbiór jedynek (łańcuchowi $\{x_i, y_j\}$ odpowiada $a_{ij} = 1$). Oczywiście rozkład zbioru P na minimalną liczbę łańcuchów rozłącznych zawiera maksymalną liczbę łańcuchów dwuelementowych. Stąd

$$k = m+n-r \tag{1.2}$$

(Zauważmy, że rozkład zbioru P na s łańcuchów zawiera zawsze $m+n-s$ łańcuchów dwuelementowych).

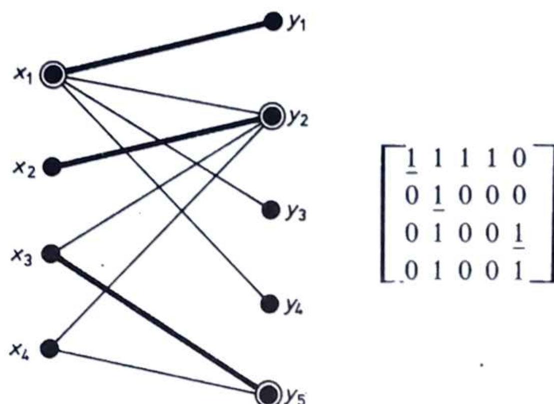
Na mocy twierdzenia Dilwortha $q = r$. Z porównania (1.1) z (1.2) otrzymujemy zatem $k = l$. □

Twierdzenie węgierskie można również sformułować w języku teorii grafów. W tym celu przyporządkujmy dowolnemu grafowi dwudzielnemu o zbiorze wierzchołków $\{x_1, \ldots, x_m\} \cup \{y_1, \ldots, y_n\}$ (w którym każda krawędź łączy pewien wierzchołek x_i z pewnym wierzchołkiem y_j) macierz zero-jedynkową $A = [a_{ij}]$ wymiaru

$m \times n$, w której $a_{ij} = 1$ wtedy i tylko wtedy, gdy $\{x_i, y_j\}$ jest krawędzią grafu. Nazwijmy *skojarzeniem* dowolny zbiór krawędzi grafu, z których żadne dwie nie są incydentne ze wspólnym wierzchołkiem (każda krawędź $\{x, y\}$ skojarzenia „kojarzy" ze sobą wierzchołki x, y), natomiast *pokryciem wierzchołkowym* dowolny zbiór S wierzchołków taki, że każda krawędź grafu jest incydentna z pewnym wierzchołkiem z S. W tych terminach twierdzenie węgierskie przyjmuje postać:

Twierdzenie 1.7. *W dowolnym grafie dwudzielnym maksymalna liczność skojarzenia jest równa minimalnej liczności pokrycia wierzchołkowego.* □

Zilustrowano to na rys. 20.



Rys. 20. Ilustracja twierdzenia węgierskiego. Grubszą linią zaznaczono pewne skojarzenie o maksymalnej liczności, natomiast kółkami pewne pokrycie wierzchołkowe o minimalnej liczności

Istnieje wiele innych twierdzeń minimaksowych związanych z grafami. Do najbardziej znanych należy twierdzenie Mengera [1] i ściśle z nim związana teoria przepływów w sieciach. Zainteresowanego Czytelnika odsyłamy do monografii Forda i Fulkersona [1].

§ 2. Dualność twierdzeń minimaksowych, grafy doskonałe

Nietrudno jest wykazać prawdziwość następującego twierdzenia „dualnego" względem twierdzenia węgierskiego: W dowolnej macierzy zero-jedynkowej minimalna liczba zbiorów rozproszonych pokrywających wszystkie jedynki jest równa maksymalnej liczbie jedynek w linii. W paragrafie tym zdefiniujemy ściśle, w przypadku znacznie ogólniejszych twierdzeń minimaksowych, na czym polega powyższa dualność, oraz podamy pewne ogólne twierdzenie pozwalające automatycznie wnioskować o prawdziwości twierdzenia „dualnego" na podstawie prawdziwości twierdzenia „prostego".

Niech X będzie dowolnym zbiorem skończonym i niech $\mathscr{A} \subseteq \mathscr{P}(X)$. O zbiorze $B \subseteq X$ powiemy, że jest *rozproszony* w $\mathscr{A}$, jeśli $|A \cap B| \leqslant 1$ dla każdego $A \in \mathscr{A}$.

Oznaczmy przez $\mathscr{A}^*$ rodzinę wszystkich zbiorów $B \subseteq X$ rozproszonych w $\mathscr{A}$. Łatwo zauważyć, że każdy zbiór $A \in \mathscr{A}$ jest rozproszony w $\mathscr{A}^*$, tzn. $\mathscr{A} \subseteq \mathscr{A}^{**}$. Nas będą interesowały rodziny $\mathscr{A}$ o tej własności, że $\mathscr{A}$ jest rodziną wszystkich zbiorów rozproszonych w $\mathscr{A}^*$, innymi słowy $\mathscr{A} = \mathscr{A}^{**}$. Rodziny o tej własności będziemy nazywali *refleksywnymi*.

Zbiór $A \subseteq X$ wierzchołków grafu $G = \langle X, E \rangle$ nazywamy *kliką* w G, jeśli każde dwa wierzchołki tego zbioru są połączone krawędzią grafu, tzn. jeśli $\mathscr{P}_2(A) \subseteq E$. Zbiór $B \subseteq X$ nazywamy *antykliką* w G, jeśli żadne dwa wierzchołki tego zbioru nie są połączone krawędzią grafu, tzn. jeśli $\mathscr{P}_2(A) \cap E = \emptyset$.

Podamy teraz charakteryzację refleksywnych rodzin zbiorów.

TWIERDZENIE 2.1. *Niech X będzie dowolnym zbiorem skończonym i niech $\mathscr{A} \subseteq \mathscr{P}(X)$. Następujące warunki są równoważne:*

(a) *rodzina $\mathscr{A}$ jest refleksywna,*

(b) *dla dowolnego $A \subseteq X$*

$$A \in \mathscr{A} \Leftrightarrow \mathscr{P}_2(A) \subseteq \mathscr{A},$$

(c) *$\mathscr{A}$ jest rodziną wszystkich klik pewnego grafu,*

(d) *$\mathscr{A}$ jest rodziną wszystkich antyklik pewnego grafu.*

Dowód. (a) $\Rightarrow$ (b). Załóżmy, że $\mathscr{A} = \mathscr{A}^{**}$. Wtedy $A \in \mathscr{A}$ oznacza, że A jest rozproszony w $\mathscr{A}^*$. Lecz dowolny podzbiór zbioru rozproszonego — w szczególności dowolny podzbiór dwuelementowy zbioru rozproszonego — jest rozproszony, a więc

$$A \in \mathscr{A} \Rightarrow \mathscr{P}_2(A) \subseteq \mathscr{A}.$$

Również

$$\mathscr{P}_2(A) \subseteq \mathscr{A} \Rightarrow A \in \mathscr{A},$$

gdyż jeśli $A \notin \mathscr{A} = \mathscr{A}^{**}$, to $|A \cap B| \geqslant 2$ dla pewnego $B \in \mathscr{A}^*$ i tym samym A zawiera pewien podzbiór dwuelementowy, który nie jest rozproszony w $\mathscr{A}^*$, a więc $\mathscr{P}_2(A) \nsubseteq \mathscr{A}$.

(b) $\Rightarrow$ (c). Załóżmy, że spełniony jest warunek (b) i rozważmy graf $G(\mathscr{A}) = \langle X, \mathscr{A} \cap \mathscr{P}_2(X) \rangle$. Łatwo zauważyć, że $\mathscr{A}$ jest rodziną wszystkich klik grafu $G(\mathscr{A})$. Wynika to z oczywistego faktu, że zbiór $A \subseteq X$ jest kliką wtedy i tylko wtedy, gdy każdy jego podzbiór dwuelementowy jest kliką.

(c) $\Rightarrow$ (d). Jeśli $\mathscr{A}$ jest rodziną wszystkich klik w $G = \langle X, E \rangle$, to łatwo zauważyć, że $\mathscr{A}$ jest rodziną wszystkich antyklik w dopełnieniu $\bar{G} = \langle X, \mathscr{P}_2(X) \setminus E \rangle$ grafu G.

(d) $\Rightarrow$ (a). Niech $\mathscr{A}$ będzie rodziną wszystkich antyklik w $G = \langle X, E \rangle$. Zauważmy, że zbiory rozproszone w $\mathscr{A}$ to dokładnie kliki w G, czyli antykliki w $\bar{G}$. Na tej samej zasadzie zbiory rozproszone w $\mathscr{A}^*$ to dokładnie antykliki w $\bar{\bar{G}} = G$. Tak więc $\mathscr{A}^{**} = \mathscr{A}$. □

Niech $\mathscr{A}$ będzie dowolną refleksywną rodziną podzbiorów zbioru X. Będziemy mówili, że dla rodziny $\mathscr{A}$ zachodzi *twierdzenie węgierskie*, jeśli dla każdego zbioru $Y \subseteq X$ minimalna liczba zbiorów z $\mathscr{A}$, które pokrywają Y, jest równa maksymalnej liczności zbioru rozproszonego w $\mathscr{A}$ zawartego w Y. Związek tej definicji z klasycznym twierdzeniem węgierskim jest następujący. Niech X będzie zbiorem pozycji pewnej macierzy wymiaru $m \times n$, tzn. $X = \{1, \ldots, m\} \times \{1, \ldots, n\}$, i niech $\mathscr{A}$ będzie rodziną wszystkich linii oraz wszystkich podzbiorów linii. Z twierdzenia 2.1 łatwo wynika, że rodzina $\mathscr{A}$ jest refleksywna, przy czym $\mathscr{A}^*$ jest rodziną wszystkich rozproszonych zbiorów pozycji naszej macierzy, tzn. zbiorów pozycji, z których żadne dwie nie leżą na tej samej linii. Jeśli teraz zbiór $Y \subseteq X$ interpretujemy jako zbiór (wystąpień) jedynek w naszej macierzy (w pozostałych pozycjach występują zera), to twierdzenie węgierskie dla $\mathscr{A}$ wyraża po prostu klasyczne twierdzenie węgierskie dla dowolnych macierzy zero-jedynkowych wymiaru $m \times n$. Zauważmy, że twierdzenie dualne względem klasycznego twierdzenia węgierskiego to nic innego jak twierdzenie węgierskie dla $\mathscr{A}^*$.

Podamy jeszcze jeden przykład. Niech $\langle X, \leqslant \rangle$ będzie dowolnym skończonym zbiorem częściowo uporządkowanym i niech $\mathscr{A}$ będzie rodziną wszystkich łańcuchów w $\langle X, \leqslant \rangle$. Łatwo zauważyć, że rodzina $\mathscr{A}$ jest refleksywna, przy czym $\mathscr{A}^*$ jest rodziną wszystkich antyłańcuchów w $\langle X, \leqslant \rangle$. Twierdzenie węgierskie dla $\mathscr{A}$ to nic innego jak twierdzenie Dilwortha (dla dowolnego zbioru $Y \subseteq X$ z porządkiem dziedziczonym z $\langle X, \leqslant \rangle$), natomiast dualne względem niego twierdzenie węgierskie dla $\mathscr{A}^*$ odpowiada twierdzeniu 1.2.

Przyjrzyjmy się teraz jak wygląda twierdzenie węgierskie, jeśli rodzinę refleksywną $\mathscr{A}$ reprezentujemy, zgodnie z twierdzeniem 2.1, jako rodzinę klik względnie rodzinę antyklik w pewnym grafie. Będziemy w tym celu potrzebowali paru definicji dotyczących grafów. Niech $G = \langle X, E \rangle$, $E \subseteq \mathscr{P}_2(X)$ będzie dowolnym grafem i niech $Y \subseteq X$. Przypomnijmy, że przez G_Y oznaczamy podgraf grafu G indukowany przez Y, tzn. $G_Y = \langle Y, E \cap \mathscr{P}_2(Y) \rangle$. Wprowadźmy następujące oznaczenia:

$\omega(G)$ = maksymalna liczność kliki w G,

$\chi(G)$ = minimalna liczba antyklik, które pokrywają X,

$\alpha(G)$ = maksymalna liczność antykliki w G,

$\theta(G)$ = minimalna liczba klik, które pokrywają X.

Zauważmy, że $\alpha(G) = \omega(\bar{G})$, $\theta(G) = \chi(\bar{G})$. Wielkość $\chi(G)$ nazywamy *liczbą chromatyczną* grafu G. Jest ona równa minimalnej liczbie kolorów, jakimi można pokolorować wierzchołki grafu tak, by żadna krawędź grafu nie łączyła wierzchołków tego samego koloru (o „pokolorowaniu wierzchołków grafu" będziemy zawsze milcząco zakładali ten ostatni warunek). Aby się o tym przekonać, wystarczy zauważyć, że dla każdego takiego pokolorowania $C\colon X \to \{1, \ldots, k\}$ mamy $X = C^{-1}(1) \dot\cup \ldots \dot\cup C^{-1}(k)$, przy czym każdy ze zbiorów $C^{-1}(i)$ jest antykliką; na odwrót, mając dane pokrycie zbioru X k antyklikami, łatwo jest skonstruować odpowiednie pokolorowanie wierzchołków grafu k kolorami.

Jeśli refleksywna rodzina zbiorów $\mathscr{A} \subseteq \mathscr{P}(X)$ jest reprezentowana jako rodzina

antyklik pewnego grafu G, to twierdzenie węgierskie dla $\mathscr{A}$ przyjmuje postać

(2.1) $$\chi(G_Y) = \omega(G_Y) \quad \text{dla każdego } Y \subseteq X.$$

Grafy spełniające powyższy warunek zwane są *grafami doskonałymi*. Z kolei dualne twierdzenie, tzn. twierdzenie węgierskie dla $\mathscr{A}^*$, orzeka, iż

(2.2) $$\theta(G_Y) = \alpha(G_Y) \quad \text{dla każdego } Y \subseteq X.$$

Wynika to po prostu z faktu, iż $\mathscr{A}^*$ jest rodziną wszystkich klik grafu G. Równoważnie możemy warunek (2.2) zapisać jako

(2.3) $$\chi(\bar{G}_Y) = \omega(\bar{G}_Y) \quad \text{dla każdego } Y \subseteq X.$$

C. Berge wyraził na początku lat sześćdziesiątych przypuszczenie, iż warunki (2.1) i (2.2) są równoważne dla dowolnego grafu G:

Przypuszczenie Berge'a o grafach doskonałych. Graf G jest doskonały wtedy i tylko wtedy, gdy graf $\bar{G}$ jest doskonały.

Przypuszczenie to zostało znacznie później udowodnione przez Lovásza [1, 2]. Pozostałą część tego paragrafu poświęcimy na podanie tego dowodu (por. Graver i Watkins [1]).

Niech $G = \langle X, E\rangle$ będzie dowolnym grafem i rozważmy dowolną funkcję $f\colon Z \to X$. Przez $f^{-1}(G)$ będziemy oznaczali graf o zbiorze wierzchołków Z i zbiorze krawędzi

$$\{\{x, y\} \in \mathscr{P}_2(Z)\colon f(x) = f(y) \vee \{f(x), f(y)\} \in E\}.$$

Intuicyjnie, graf $f^{-1}(G)$ powstaje przez zastąpienie każdego z wierzchołków $x \in X$ przez klikę o liczności $|f^{-1}(x)|$ i połączenie wszystkich wierzchołków kliki powstałej z x ze wszystkimi wierzchołkami kliki powstałej z y dla każdej krawędzi $\{x, y\} \in E$. Zauważmy, że zbiór $K \subseteq Z$ jest kliką w $f^{-1}(G)$ wtedy i tylko wtedy, gdy zbiór $f(K)$ jest kliką w G, oraz że jeśli A jest antykliką w $f^{-1}(G)$, to $f(A)$ jest antykliką w G i $|f(A)| = |A|$. Wynika stąd, iż

(2.4) $$\alpha\big(f^{-1}(G)\big) \leqslant \alpha(G).$$

LEMAT 2.2. *Jeśli graf $G = \langle X, E\rangle$ jest doskonały, to dla dowolnego zbioru skończonego Z i dowolnej funkcji $f\colon Z \to X$ graf $f^{-1}(G)$ jest doskonały.*

Dowód. Stosujemy indukcję względem $|Z|$. Dla $|Z| = 1$ lemat jest oczywiście prawdziwy. Niech więc $|Z| > 1$ i rozważmy graf $f^{-1}(G)$ dla pewnej funkcji $f\colon Z \to X$. Jeśli funkcja f jest różnowartościowa, to graf $f^{-1}(G)$ jest izomorficzny z $G_{f(Z)}$, który to graf jest oczywiście doskonały, jako podgraf indukowany grafu doskonałego. Załóżmy więc, że $f(x) = f(y)$ dla pewnych $x, y \in Z$, $x \neq y$, i oznaczmy $H = f^{-1}(G)$. Na mocy założenia indukcyjnego graf H_T jest doskonały dla dowolnego podzbioru właściwego $T \subset Z$ (zauważmy, że $H_T = g^{-1}(G)$, gdzie $g = f \restriction T$). Dla dowodu doskonałości grafu H wystarczy więc wykazać równość $\chi(H) = \omega(H)$. Przyjmijmy $T = Z \setminus \{x\}$ i rozważmy graf H_T.

Przypuśćmy najpierw, że y należy do pewnej kliki K o maksymalnej liczności w grafie H_T. Wówczas $K \cup \{x\}$ jest oczywiście kliką o maksymalnej liczności w H, czyli $\omega(H) = \omega(H_T)+1$. Z drugiej strony, dowolne pokolorowanie wierzchołków grafu H_T minimalną liczbą kolorów możemy rozszerzyć do pokolorowania grafu H przypisując wierzchołkowi x nowy kolor. Stąd $\chi(H) \leqslant \chi(H_T)+1$ i wobec oczywistej nierówności $\chi(H) \geqslant \omega(H)$ (każdy wierzchołek kliki musi być pokolorowany innym kolorem) oraz równości $\chi(H_T) = \omega(H_T)$ (założenie indukcyjne) otrzymujemy $\chi(H) = \omega(H)$.

Przejdźmy teraz do przypadku, gdy y nie należy do żadnej kliki o maksymalnej liczności w grafie H_T. Niech $C\colon T \to \{1, \ldots, \chi(H_T)\}$ będzie pokolorowaniem wierzchołków grafu H_T minimalną liczbą kolorów i przyjmijmy, bez zmniejszenia ogólności, że $C(y) = 1$. Z równości $\chi(H_T) = \omega(H_T)$ łatwo wynika, że antyklika $C^{-1}(1)$ przecina każdą klikę o maksymalnej liczności w H_T. Lecz wobec naszego założenia o wierzchołku y tę samą własność ma również mniejsza antyklika $A = C^{-1}(1)\setminus\{y\}$. Stąd $\omega(H_{T\setminus A}) = \omega(H_T)-1$ i wobec doskonałości grafu $H_{T\setminus A}$ również $\chi(H_{T\setminus A}) = \omega(H_T)-1$. Zauważmy, że zbiór $A \cup \{x\} = (C^{-1}(1)\setminus\{y\}) \cup \{x\}$ jest antykliką w H (gdyż $C^{-1}(1)$ jest antykliką, a z równości $f(x) = f(y)$ wynika, że wierzchołki x, y są połączone z dokładnie tymi samymi wierzchołkami w zbiorze $Z\setminus\{x, y\}$). Tak więc dowolne pokolorowanie wierzchołków grafu $H_{T\setminus A}$ $\omega(H_T)-1$ kolorami można uzupełnić do pokolorowania wierzchołków grafu $H_{(T\setminus A)\cup A\cup\{x\}} = H_Z = H$ $\omega(H_T)$ kolorami. Stąd $\chi(H) \leqslant \omega(H_T) \leqslant \omega(H)$ i wobec oczywistej nierówności $\omega(H) \leqslant \chi(H)$ otrzymujemy $\chi(H) = \omega(H)$. □

Klikę w grafie G będziemy nazywali *regularną*, jeśli ma ona niepuste przecięcie z każdą antykliką o maksymalnej liczności w G. Podobnie antyklikę w grafie G będziemy nazywali *regularną*, jeśli ma ona niepuste przecięcie z każdą kliką o maksymalnej liczności w G, tzn. jeśli jest ona kliką regularną w $\bar{G}$.

TWIERDZENIE 2.3 (Lovász [1, 2]). *Dla dowolnego grafu $G = \langle X, E\rangle$ następujące warunki są równoważne:*

(a) *graf G jest doskonały,*

(b) *graf $\bar{G}$ jest doskonały,*

(c) *graf G_Y zawiera klikę regularną dla dowolnego $Y \subseteq X$,*

(d) *graf G_Y zawiera antyklikę regularną dla dowolnego $Y \subseteq X$.*

Dowód. (a)$\Rightarrow$(c). Stosujemy indukcję względem $|X|$. Dla $|X| = 1$ nasza implikacja jest oczywista. Załóżmy więc, że $n = |X| > 1$, że graf $G = \langle X, E\rangle$ jest doskonały, i że wynikanie (a)$\Rightarrow$(c) jest prawdziwe dla wszystkich grafów o mniej niż n wierzchołkach. Wynika stąd, że dla każdego podzbioru właściwego $Y \subsetneq X$ graf G_Y — który jest oczywiście doskonały — zawiera klikę regularną. Przypuśćmy, że w grafie G nie istnieje klika regularna. Wykażemy, że przypuszczenie to prowadzi do sprzeczności.

Niech $\mathscr{C}$ będzie rodziną wszystkich klik grafu G. Zgodnie z naszym założeniem dla każdej kliki $K \in \mathscr{C}$ istnieje antyklika A_K o maksymalnej liczności — równej $\alpha(G)$— taka, że $K \cap A_K = \emptyset$. Rozważmy dla każdej takiej kliki K zbiór $\alpha(G)$-

elementowy Z_K ($Z_{K_1} \cap Z_{K_2} = \emptyset$ dla $K_1 \neq K_2$) i oznaczmy $Z = \bigcup_{K \in \mathscr{C}} Z_K$. Zdefiniujmy funkcję f: $Z \to X$ tak, by $f(Z_K) = A_K$ dla każdej kliki $K \in \mathscr{C}$ (tzn. $f \upharpoonright Z_K$ jest odwzorowaniem wzajemnie jednoznacznym Z_K na A_K). Zgodnie z lematem 2.2 graf $H = f^{-1}(G)$ jest doskonały. Niech C będzie dowolną kliką w H. Wówczas $f(C)$ jest kliką w G i wobec $f(C) \cap A_{f(C)} = \emptyset$ otrzymujemy

(2.5) $$C \cap Z_{f(C)} = \emptyset.$$

Lecz Z_K jest antykliką w H dla każdego $K \in \mathscr{C}$ i co za tym idzie $|C \cap Z_K| \leqslant 1$. Tak więc (2.5) oznacza, iż $|C| < |\mathscr{C}|$, i w konsekwencji $\omega(H) < |\mathscr{C}|$. Zauważmy, że

(2.6) $$\chi(H)\alpha(H) \geqslant |Z|,$$

jako że pokolorowanie grafu $H\chi(H)$ kolorami określa podział zbioru jego wierzchołków na $\chi(H)$ antyklik, każda o liczności nie przekraczającej $\alpha(H)$. Korzystając z faktu, iż graf H jest doskonały i z (2.4) otrzymujemy ostatecznie

$$\chi(H)\alpha(H) = \omega(H)\alpha(H) < |\mathscr{C}|\,\alpha(G) = |Z|,$$

co w połączeniu z (2.6) daje zapowiedzianą sprzeczność. Tak więc G musi zawierać klikę regularną, co kończy dowód wynikania (a)$\Rightarrow$(c).

(c)$\Rightarrow$(b) Załóżmy, że graf G_Y zawiera klikę regularną dla dowolnego $Y \subseteq X$. Wtedy graf $\bar{G}_Y$ zawiera oczywiście antyklikę regularną dla dowolnego $Y \subseteq X$. Wykażemy, że graf $\bar{G}$ jest doskonały. Stosujemy indukcję względem $|X|$. Jest to oczywiście prawdą dla $|X| = 1$, niech więc $|X| > 1$. Na mocy założenia indukcyjnego graf $\bar{G}_Y$ jest doskonały dla każdego podzbioru właściwego $Y \subset X$ (gdyż $|Y| < |X|$ oraz graf $\bar{G}_T$ zawiera antyklikę regularną dla każdego $T \subseteq Y$). Wystarczy zatem wykazać, że $\chi(\bar{G}) = \omega(\bar{G})$. Niech A będzie dowolną antykliką regularną w $\bar{G}$. Wtedy oczywiście $\omega(\bar{G}_{X\setminus A}) = \omega(\bar{G}) - 1$ oraz $\chi(\bar{G}) \leqslant \chi(\bar{G}_{X\setminus A}) + 1$, jako że dowolne pokolorowanie grafu $\bar{G}_{X\setminus A}$ może być rozszerzone do pokolorowania całego grafu $\bar{G}$ przez nadanie nowego koloru wierzchołkom antykliki A. Korzystając z doskonałości grafu $\bar{G}_{X\setminus A}$ otrzymujemy

$$\chi(\bar{G}) \leqslant \chi(\bar{G}_{X\setminus A}) + 1 = \omega(\bar{G}_{X\setminus A}) + 1 = \omega(\bar{G}),$$

co w połączeniu z oczywistą nierównością $\omega(\bar{G}) \leqslant \chi(\bar{G})$ daje żądaną równość $\chi(\bar{G}) = \omega(\bar{G})$.

(b)$\Rightarrow$(d) otrzymujemy z implikacji (a)$\Rightarrow$(c) przez zamianę grafu G na $\bar{G}$, i w podobny sposób (d)$\Rightarrow$(a) otrzymujemy z implikacji (c)$\Rightarrow$(b). □

Odnotujmy zapowiadany już wniosek z twierdzenia 2.3.

WNIOSEK 2.4. *Twierdzenie węgierskie dla danej refleksywnej rodziny zbiorów $\mathscr{A}$ zachodzi wtedy i tylko wtedy, gdy zachodzi dla $\mathscr{A}^*$.* □

Znanych jest wiele klas grafów doskonałych, nie podano natomiast dotychczas żadnej prostej ogólnej charakteryzacji takich grafów. Na zakończenie tego paragrafu warto przytoczyć następujące, dotychczas nie rozstrzygnięte

Silne przypuszczenie Berge'a o grafach doskonałych. Graf G jest doskonały wtedy i tylko wtedy, gdy ani G, ani $\bar{G}$ nie zawiera podgrafu indukowanego izomorficznego z cyklem elementarnym nieparzystej długości większej od 3.

Powyższy warunek jest oczywiście konieczny, jako że dla grafu C postaci cyklu elementarnego nieparzystej długości większej od 3 mamy $\chi(C) = 3 \neq \omega(C) = 2$.

Czytelnika pragnącego głębiej poznać zagadnienia związane z grafami doskonałymi odsyłamy do zbioru artykułów pod redakcją Berge'a i Chvátala [1].

§ 3. Ekstremalne własności rodzin zbiorów, twierdzenie Spernera

Przyjrzyjmy się co mówi twierdzenie Dilwortha w przypadku zbioru częściowo uporządkowanego $\langle \mathscr{P}(X), \subseteq \rangle$ – rodziny wszystkich podzbiorów pewnego zbioru skończonego X, uporządkowanej przez zawieranie. Antyłańcuchy w takim zbiorze będziemy nazywali *rodzinami Spernera.* Najprostszą rodziną Spernera, jaka przychodzi na myśl, jest rodzina $\mathscr{P}_k(x)$ wszystkich podzbiorów k-elementowych zbioru X dla pewnego $k \leqslant n = |X|$. Liczność takiej rodziny wynosi $\binom{n}{k}$. Współczynnik $\binom{n}{k}$ osiąga maksimum dla $k = \lfloor n/2 \rfloor$ (lub dla $k = \lfloor n/2 \rfloor$ i $k = \lceil n/2 \rceil$, jeśli n jest nieparzyste, por. rozdz. 1, zadanie 47), tak więc istnieje rodzina Spernera o liczności $\binom{n}{\lfloor n/2 \rfloor}$. Okazuje się, że jest to maksymalna liczność rodziny Spernera podzbiorów zbioru n-elementowego. Fakt ten otrzymamy jako wniosek z następującego twierdzenia udowodnionego niezależnie przez Lubella [1], Meshalkina [1] i Yamamoto [1]:

TWIERDZENIE 3.1. *Niech $\{A_1, \ldots, A_m\}$ będzie rodziną Spernera podzbiorów zbioru n-elementowego X. Wówczas*

$$\sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1.$$

Dowód (Lubell [1]). Nazwijmy *łańcuchem zupełnym* każdy łańcuch postaci $\emptyset = C_0 \subset C_1 \subset \ldots \subset C_n = X$ $(|C_i| = i$ dla $0 \leqslant i \leqslant n)$. Wszystkich łańcuchów zupełnych jest $n!$ (C_1 można wybrać na n sposobów, C_2 – przy ustalonym C_1 – na $n-1$ sposobów itd.). Rozumując podobnie widzimy, że zbiór A_i jest elementem $|A_i|!(n-|A_i|)!$ łańcuchów zupełnych. Istotnie, jeśli $C_{|A_i|} = A_i$, to mamy $|A_i|!$ sposobów wybrania zbiorów $C_0, C_1, \ldots, C_{|A_i|-1}$, zaś zbiory $C_{|A_i|+1}, \ldots, C_n$ możemy wybrać na $(n-|A_i|)!$ sposobów. Rodzina $\{A_1, \ldots, A_m\}$ jest antyłańcuchem, zatem każdy łańcuch zawiera najwyżej jeden spośród zbiorów $A_1, \ldots, A_m$. Stąd liczba łańcuchów zupełnych przecinających zbiór $\{A_1, \ldots, A_m\}$ jest równa

$\sum_{i=1}^{m} |A_i|!(n-|A_i|)!$. Przyrównując tę liczbę do liczby wszystkich łańcuchów zupełnych otrzymujemy nierówność

$$\sum_{i=1}^{m} |A_i|!(n-|A_i|)! \leqslant n!,$$

czyli

$$\sum_{i=1}^{m} \frac{|A_i|!(n-|A_i|)!}{n!} = \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1. \quad \Box$$

Inny dowód twierdzenia 3.1 można znaleźć w pracy Frankla [1].

Wobec $\binom{n}{|A_i|} \leqslant \binom{n}{\lfloor n/2 \rfloor}$ mamy

$$m \frac{1}{\binom{n}{\lfloor n/2 \rfloor}} \leqslant \sum_{i=1}^{m} \frac{1}{\binom{n}{|A_i|}} \leqslant 1,$$

i w konsekwencji otrzymujemy zapowiedziane już

TWIERDZENIE 3.2 (Sperner [1]). *Jeśli $\mathscr{A}$ jest rodziną Spernera podzbiorów zbioru n-elementowego, to*

$$|\mathscr{A}| \leqslant \binom{n}{\lfloor n/2 \rfloor}. \quad \Box$$

Oczywiście twierdzenie 3.1 mówi nam znacznie więcej o strukturze rodzin Spernera niż twierdzenie 3.2.

Z twierdzenia Dilwortha wynika, że $\mathscr{P}(X)$ można przedstawić w postaci sumy $\binom{n}{\lfloor n/2 \rfloor}$ łańcuchów rozłącznych. Choć samo twierdzenie Dilwortha, ani też jego dowód, nie dają żadnej prostej metody wyznaczania takiego rozkładu, metoda taka jest znana (p. np. Greene i Kleitman [1]). Aby ją opisać, nazwijmy łańcuch w $\mathscr{P}(X)$ *symetrycznym*, jeśli jest on postaci

$$C_{\lfloor n/2 \rfloor - j} \subset C_{\lfloor n/2 \rfloor - j+1} \subset \ldots \subset C_{\lceil n/2 \rceil + j},$$

gdzie $|C_i| = i$ dla $\lfloor n/2 \rfloor - j \leqslant i \leqslant \lceil n/2 \rceil + j$ ($n = |X|$, $j \geqslant 0$). Każdy łańcuch symetryczny zawiera dokładnie jeden zbiór liczności $\lfloor n/2 \rfloor$, tak więc każdy rozkład rodziny $\mathscr{P}(X)$ na sumę parami rozłącznych (niepustych) łańcuchów symetrycznych jest automatycznie rozkładem na $\binom{n}{\lfloor n/2 \rfloor}$ takich łańcuchów. Rozkład taki konstruujemy indukcyjnie względem $|X|$. Dla $|X| = 1$ rodzina $\mathscr{P}(X) = \{\emptyset; X\}$ sama jest łańcuchem symetrycznym. Załóżmy, że mamy już rozkład rodziny $\mathscr{P}(X)$; chcemy wyznaczyć rozkład rodziny $\mathscr{P}(X \cup \{a\})$ ($a \notin X$). W tym celu przyporządko-

wujemy każdemu łańcuchowi $A_1 \subset \ldots \subset A_k$ naszego rozkładu dwa łańcuchy

$$A_1 \subset \ldots \subset A_k, \qquad A_1 \cup \{a\} \subset \ldots \subset A_k \cup \{a\}.$$

Żaden z tych łańcuchów nie jest symetryczny w $\mathscr{P}(X \cup \{a\})$, lecz oba stają się symetryczne, jeśli przeniesiemy element maksymalny drugiego łańcucha do pierwszego:

$$A_1 \subset \ldots \subset A_k \subset A_k \cup \{a\}, \qquad A_1 \cup \{a\} \subset \ldots \subset A_{k-1} \cup \{a\}$$

(jeśli $k = 1$, to otrzymujemy tylko jeden łańcuch symetryczny, gdyż drugi staje się pusty). Postępując tak ze wszystkimi łańcuchami z rozkładu rodziny $\mathscr{P}(X)$ otrzymujemy rozkład rodziny $\mathscr{P}(X \cup \{a\})$ na łańcuchy symetryczne. Zauważmy, że konstrukcja ta stanowi niezależny dowód twierdzenia Spernera.

Twierdzenia 3.1 i 3.2 można uogólnić również na inne zbiory częściowo uporządkowane, na przykład na kratę $\mathscr{L}(n, q)$ wszystkich podprzestrzeni n-wymiarowej przestrzeni liniowej nad ciałem $GF(q)$ (q jest potęgą liczby pierwszej). Przypomnijmy, że przez $\binom{n}{k}_q$ oznaczamy liczbę podprzestrzeni k-wymiarowych takiej przestrzeni (por. rozdział 1, § 12). Stosując identyczną metodę jak w dowodzie twierdzenia 3.1 otrzymujemy

TWIERDZENIE 3.3. *Niech* $\{L_1, \ldots, L_m\} \subseteq \mathscr{L}(n, q)$ *i niech* $L_i \nsubseteq L_j$ *dla* $i \neq j$, $1 \leqslant i$, $j \leqslant n$. *Wówczas*

$$\sum_{i=1}^{m} \frac{1}{\binom{n}{\dim L_i}_q} \leqslant 1.$$

Dowód. Wszystkich łańcuchów postaci $\{0\} = C_0 \subset C_1 \subset \ldots \subset C_n$ (gdzie C_i jest podprzestrzenią i-wymiarową, $1 \leqslant i \leqslant n$) jest $(q^n - 1)\ (q^n - q) \ldots (q^n - q^{n-1})$. Łańcuchów takich zawierających L_i jest

$$(q^k - 1)(q^k - q) \ldots (q^k - q^{k-1}) \cdot (q^n - q^k)(q^n - q^{k+1}) \ldots (q^n - q^{n-1}),$$

gdzie $k = \dim L_i$. Mamy więc

$$\sum_{i=1}^{m} (q^{k_i} - 1)(q^{k_i} - q) \ldots (q^{k_i} - q^{k_i - 1}) \cdot (q^n - q^{k_i})(q^n - q^{k_i + 1}) \ldots (q^n - q^{n-1}) \leqslant$$

$$\leqslant (q^n - 1)(q^n - q) \ldots (q^n - q^{n-1}),$$

czyli

$$\sum_{i=1}^{m} \frac{(q^{k_i} - 1)(q^{k_i} - q) \ldots (q^{k_i} - q^{k_i - 1})}{(q^n - 1)(q^n - q) \ldots (q^n - q^{k_i - 1})} = \sum_{i=1}^{m} \frac{1}{\binom{n}{k_i}_q} \leqslant 1,$$

gdzie $k_i = \dim L_i$. □

Biorąc pod uwagę, że $\max_{1 \leqslant i \leqslant n} \binom{n}{i}_q = \binom{n}{\lfloor n/2 \rfloor}_q$ (por. rozdz. 1, zadanie 74) otrzymujemy następujący odpowiednik twierdzenia Spernera:

Twierdzenie 3.4. *Niech* $\{L_1, \ldots, L_m\} \subseteq \mathscr{L}(n, q)$ *i niech* $L_i \nsubseteq L_j$ *dla* $i \neq j$, $1 \leqslant i, j \leqslant m$. *Wówczas*

$$m \leqslant \binom{n}{\lfloor n/2 \rfloor}_q . \ \square$$

Zauważmy, że w przypadku zbiorów $\mathscr{P}(X)$ i $\mathscr{L}(n, q)$ z porządkiem częściowym określonym przez inkluzję, antyłańcuch o maksymalnej liczności możemy zawsze znaleźć w postaci warstwy elementów o jednakowej randze. Interesujący jest fakt, iż dla dużych n własność ta nie przysługuje zbiorowi $\Pi(X)$ podziałów zbioru n-elementowego X częściowo uporządkowanemu przez relację rozdrobnienia (Canfield [1]).

Interesującym problemem jest określanie maksymalnej liczności rodziny zbiorów (podprzestrzeni przestrzeni liniowej itp.) rozpatrując zamiast $A_i \nsubseteq A_j$ $(i \neq j)$ inne ograniczenia, np. $A_i \cap A_j \neq \emptyset$, $A_i \cup A_j \neq X$, $|A_i \cap A_j| \geqslant k$ dla pewnego k, lub też kombinacje tych warunków. Jeszcze innym typem ograniczenia jest żądanie, by rodzina nie zawierała łańcucha (antyłańcucha) o $r+1$ elementach. Czytelnika zainteresowanego tego typu zagadnieniami odsyłamy do przeglądowej pracy Erdösa i Kleitmana [1] (p. też zadania). Udowodnimy tu jedynie jedno z ważniejszych twierdzeń tego typu, pochodzące od Erdösa, Ko i Rado [1] i dotyczące rodzin Spernera, w których żadne dwa zbiory nie są rozłączne. Jeśli n jest nieparzyste, to oczywiście $\mathscr{P}_{\lceil n/2 \rceil}(X)$, $|X| = n$ jest taką rodziną, gdyż dla dowolnych $A, B \in \mathscr{P}_{\lceil n/2 \rceil}(X)$ mamy $|A|+|B| = n+1$ i w konsekwencji $A \cap B \neq \emptyset$. Jeśli wprowadzimy dodatkowe ograniczenie $|A| \leqslant k$ dla każdego $A \in \mathscr{A}$, gdzie $k \leqslant n/2$, to przykładem rodziny Spernera $\mathscr{A}$ nie zawierającej zbiorów rozłącznych jest, przy dowolnym n, rodzina

$$\mathscr{A} = \{B \cup \{a\} \colon B \in \mathscr{P}_{k-1}(X \setminus \{a\})\}, \qquad |X| = n, \ a \in X$$

o liczności $\binom{n-1}{k-1}$. Wykażemy w dalszym ciagu, że jest to w istocie maksymalna możliwa liczność rodziny Spernera spełniającej powyższe ograniczenia.

Niech $\emptyset \neq A \subseteq X$, gdzie $|X| = n$, oraz niech $\langle x_0, \ldots, x_{n-1} \rangle$ będzie ciągiem różnowartościowym elementów zbioru X. Będziemy mówili, że A jest *odcinkiem* w $\langle x_0, \ldots, x_{n-1} \rangle$, jeśli $A = \{x_i, x_{i+1}, \ldots, x_{i+|A|-1}\}$ dla pewnego i, gdzie wskaźniki obliczane są modulo n. Jednoznacznie wyznaczone przez A elementy x_i oraz $x_{i+|A|}$ nazywamy odpowiednio *początkiem* i *końcem* zbioru A w $\langle x_0, \ldots, x_{n-1} \rangle$ (zauważmy, że koniec, w przeciwieństwie do początku, nie należy do A).

Lemat 3.5. *Niech* $|X| = n$, *niech* $\langle x_0, \ldots, x_{n-1} \rangle$ *będzie ciągiem różnowartościowym elementów zbioru* X *oraz niech* $k \leqslant n/2$. *Wówczas dla dowolnej rodziny* $\mathscr{A} \subseteq \mathscr{P}(X)$ *spełniającej warunki*

(a) *$\mathscr{A}$ jest rodziną Spernera i $A \cap B \neq \emptyset$ dla dowolnych $A, B \in \mathscr{A}$,*
(b) *$|A| \leqslant k$ dla każdego $A \in \mathscr{A}$,*
(c) *każdy zbiór $A \in \mathscr{A}$ jest odcinkiem w $\langle x_0, \ldots, x_{n-1} \rangle$,*
mamy $|\mathscr{A}| \leqslant k$.

Dowód. Ustalmy dowolny zbiór $A \in \mathscr{A}$ i załóżmy, że

$$A = \{x_i, x_{i+1}, \ldots, x_{i+|A|-1}\}.$$

Zauważmy, że żaden element $x \in X$ nie może być wspólnym początkiem ani też wspólnym końcem dwóch różnych zbiorów z $\mathscr{A}$, gdyż wówczas jeden z tych zbiorów byłby zawarty w drugim. Żaden element nie może być również jednocześnie początkiem jednego i końcem drugiego zbioru z $\mathscr{A}$, gdyż zbiory te byłyby rozłączne. Każdy zbiór $B \in \mathscr{A}$ różny od A ma niepuste przecięcie z A, a więc jeden z $|A|-1$ elementów $x_{i+1}, \ldots, x_{i+|A|-1}$ musi być jego początkiem lub końcem. Na mocy naszych poprzednich uwag wnioskujemy, że w $\mathscr{A}$ jest co najwyżej $|A|-1$ zbiorów różnych od A. Tak więc $|\mathscr{A}| \leqslant |A| \leqslant k$. □

Korzystając z powyższego lematu możemy już łatwo udowodnić

TWIERDZENIE 3.6 (Erdös, Ko i Rado [1]; por. także Katona [1]). *Niech $\mathscr{A}$ będzie rodziną Spernera podzbiorów zbioru n-elementowego X nie zawierającą zbiorów rozłącznych i niech $|A| \leqslant k$ dla każdego $A \in \mathscr{A}$, gdzie $k \leqslant n/2$. Wówczas $|\mathscr{A}| \leqslant \binom{n-1}{k-1}$.*

Dowód. Obliczymy na dwa sposoby liczbę par postaci $\langle A, \langle x_0, \ldots, x_{n-1} \rangle \rangle$, gdzie $A \in \mathscr{A}$, $\langle x_0, \ldots, x_{n-1} \rangle$ jest dowolnym różnowartościowym ciągiem elementów zbioru X oraz A jest odcinkiem w $\langle x_0, \ldots, x_{n-1} \rangle$. Z jednej strony, dla ustalonego A liczba takich par jest równa

$$n|A|!(n-|A|)! = n \frac{n!}{\binom{n}{|A|}} \geqslant n \frac{n!}{\binom{n}{k}} = nk!(n-k)!.$$

Z drugiej strony, wobec lematu 3.5, dla każdego z $n!$ ciągów $\langle x_0, \ldots, x_{n-1} \rangle$ liczba naszych par nie przekracza k. Stąd

$$|\mathscr{A}|\, nk!(n-k)! \leqslant n!\, k,$$

czyli

$$|\mathscr{A}| \leqslant \frac{n!\,k}{nk!(n-k)!} = \frac{(n-1)!}{(k-1)!(n-k)!} = \binom{n-1}{k-1}. \quad \square$$

§ 4. Twierdzenie Halla o systemach reprezentantów

Zajmiemy się obecnie kręgiem zagadnień związanych z następującym problemem:

Dany jest ciąg $\langle A_1, \ldots, A_n \rangle$ podzbiorów (niekoniecznie różnych) pewnego

zbioru skończonego X. Czy można z każdego zbioru A_i wybrać po jednym elemencie tak, by były one parami różne? Ciąg $\langle a_1, \ldots, a_n \rangle$ taki, że $a_i \in A_i$ oraz $a_i \neq a_j$ dla $i \neq j$, $1 \leqslant i, j \leqslant n$, nazywamy *systemem reprezentantów* dla ciągu $\langle A_1, \ldots, A_n \rangle$ (a_i jest *reprezentantem* dla A_i).

Znanych jest wiele „niematematycznych" sformułowań tego problemu. Oto niektóre z nich:

1 (Problem małżeństw). W pewnej grupie dziewcząt i chłopców każdy z chłopców zna pewną liczbę dziewcząt. Czy chłopcy ci mogą wybrać sobie żony, każdy spośród dziewcząt, które zna (A_i odpowiada zbiorowi dziewcząt, które zna i-ty chłopiec)?

2 (Problem komisji). W pewnej organizacji działa n komisji, przy czym jedna osoba może być członkiem wielu komisji. Czy można z każdej komisji wyłonić przewodniczącego tak, by każda komisja miała innego przewodniczącego (A_i odpowiada zbiorowi osób zasiadających w i-tej komisji)?

3 (Problem rozdziału prac). Dana jest pewna grupa osób i pewna liczba prac. Każda z osób może mieć kwalifikacje do wykonywania wielu prac. Czy można każdej osobie przyporządkować pracę, do której ma ona kwalifikacje, tak by różnym osobom odpowiadały różne prace (A_i odpowiada zbiorowi prac, które może wykonywać i-ta osoba)?

Przykład. Rozważmy ciąg $\langle \{1, 2\}, \{2, 3\}, \{2\}, \{1, 2, 3, 4\} \rangle$. Systemem reprezentantów dla niego jest $\langle 1, 3, 2, 4 \rangle$. Łatwo sprawdzić, iż jest to jedyny system reprezentantów. Natomiast dla ciągu $\langle \{1, 2\}, \{2\}, \{1, 2\}, \{1, 2, 3, 4\} \rangle$ nie istnieje system reprezentantów. Istotnie, na reprezentantów dla pierwszych trzech zbiorów potrzebujemy trzech różnych elementów, podczas gdy zbiory te w sumie zawierają tylko dwa elementy: 1 i 2.

Uogólniając tę ostatnią obserwację, możemy sformułować następujący warunek konieczny na to, by dla ciągu $\langle A_1, \ldots, A_n \rangle$ istniał system reprezentantów:

Warunek Halla. Dla każdego zbioru $J \subseteq \{1, \ldots, n\}$

$$\left|\bigcup_{i \in J} A_i\right| \geqslant |J|.$$

Innymi słowy, dla każdego k dowolnych k spośród zbiorów A_i zawiera w sumie co najmniej k elementów.

Warunek ten jest konieczny dla istnienia systemu reprezentantów dla $\langle A_1, \ldots, A_n \rangle$, gdyż jeśli $\langle a_1, \ldots, a_n \rangle$ jest takim systemem reprezentantów, to

$$\left|\bigcup_{i \in J} A_i\right| \geqslant \left|\bigcup_{i \in J} \{a_i\}\right| = |J|.$$

Jednym z klasycznych rezultatów kombinatoryki jest fakt, iż warunek Halla jest również wystarczający dla istnienia systemu reprezentantów.

Twierdzenie 4.1 (P. Hall [1]). *Dla ciągu $\langle A_1, \ldots, A_n \rangle$ istnieje system reprezentantów wtedy i tylko wtedy, gdy dla dowolnego $J \subseteq \{1, \ldots, n\}$*

$$\left|\bigcup_{i \in J} A_i\right| \geqslant |J|.$$

Dowód (R. Rado). Wykażemy, że jeśli $\langle A_1, \ldots, A_n\rangle$ spełnia warunek Halla oraz dla pewnego i mamy $|A_i| \geqslant 2$, to istnieje taki element $x \in A_i$, że $\langle A_1, \ldots, A_i \setminus \{x\}, \ldots, A_n\rangle$ spełnia warunek Halla. Istotnie, niech $x_1, x_2 \in A_i$, $x_1 \neq x_2$. Gdyby oba ciągi $\langle A_1, \ldots, A_i \setminus \{x_k\}, \ldots, A_n\rangle$, $k = 1, 2$ nie spełniały warunku Halla, to istniałyby zbiory $J_1, J_2 \subseteq \{1, \ldots, n\}$ nie zawierające i takie, że

$$\Big|(A_i \setminus \{x_k\}) \cup \bigcup_{j\in J_k} A_j\Big| \leqslant |J_k|, \qquad k = 1, 2.$$

Oznaczając

$$S_k = (A_i \setminus \{x_k\}) \cup \bigcup_{j\in J_k} A_j, \qquad k = 1, 2$$

doszlibyśmy w następujący sposób do sprzeczności:

$$\begin{aligned}|J_1|+|J_2| &\geqslant |S_1|+|S_2| = |S_1 \cup S_2|+|S_1 \cap S_2| \geqslant \\ &\geqslant \Big|A_i \cup \bigcup_{j\in J_1\cup J_2} A_j\Big| + \Big|\big(\bigcup_{j\in J_1} A_j\big) \cap \big(\bigcup_{j\in J_2} A_j\big)\Big| \geqslant \\ &\geqslant \Big|A_i \cup \bigcup_{j\in J_1\cup J_2} A_j\Big| + \Big|\bigcup_{j\in J_1\cap J_2} A_i\Big| \geqslant \\ &\geqslant 1+|J_1 \cup J_2|+|J_1 \cap J_2| = 1+|J_1|+|J_2|.\end{aligned}$$

Zauważmy teraz, że jeśli $\langle A_1, \ldots, A_n\rangle$ spełnia warunek Halla i $|A_1|+\ldots+|A_n| = n$, to $\langle A_1, \ldots, A_n\rangle = \langle\{a_1\}, \ldots, \{a_n\}\rangle$ i $\langle a_1, \ldots, a_n\rangle$ jest żądanym systemem reprezentantów. Tak więc twierdzenie Halla otrzymujemy stosując indukcję względem $|A_1|+\ldots+|A_n|$. □

W rozdziale tym poznamy również inne dowody twierdzenia Halla (por. twierdzenia 5.1 i 8.1).

§ 5. Liczba systemów reprezentantów i permanent macierzy

Skoro wiemy już kiedy system reprezentantów istnieje, naturalne staje się pytanie, ile różnych systemów reprezentantów istnieje dla danego ciągu zbiorów. Pewnego oszacowania dolnego dostarcza nam następujące twierdzenie:

Twierdzenie 5.1 (M. Hall [2]). *Niech dla ciągu $\langle A_1, \ldots, A_n\rangle$ będzie spełniony warunek Halla i niech $|A_i| \geqslant k$ dla $1 \leqslant k \leqslant n$. Wówczas ciąg $\langle A_1, \ldots, A_n\rangle$ ma co najmniej $k!$ systemów reprezentantów, gdy $k \leqslant n$, oraz co najmniej $k!/(k-n)!$ systemów reprezentantów, gdy $k > n$.*

Dowód. Stosujemy indukcję względem n. Dla $n = 1$ twierdzenie jest w oczywisty sposób prawdziwe. Załóżmy, że twierdzenie jest prawdziwe dla dowolnych ciągów $\langle B_1, \ldots, B_m\rangle$, $m < n$. Z założenia tego wywnioskujemy prawdziwość twierdzenia dla ciągu $\langle A_1, \ldots, A_n\rangle$.

Rozważymy dwa przypadki:

Przypadek 1: $|\bigcup_{i\in J} A_i| \geqslant |J|+1$ dla każdego niepustego $J \subseteq \{1, \ldots, n-1\}$. Dla każdego $x \in A_n$ ciąg $\langle A_1 \setminus \{x\}, \ldots, A_{n-1} \setminus \{x\}\rangle$ spełnia wtedy warunek Halla, gdyż $|\bigcup_{i\in J} (A_i \setminus \{x\})| \geqslant |\bigcup_{i\in J} A_i| - 1 \geqslant |J|$. Na mocy założenia indukcyjnego istnieje $(k-1)!$ lub też $(k-1)!/((k-1)-(n-1))! = (k-1)!/(k-n)!$ systemów reprezentantów dla $\langle A_1 \setminus \{x\}, \ldots, A_{n-1} \setminus \{x\}\rangle$, w zależności od tego czy $k \leqslant n$ (czyli $k-1 \leqslant n-1$), czy też $k > n$. Lecz element $x \in A_n$ możemy wybrać na co najmniej k sposobów, stąd liczba systemów reprezentantów dla $\langle A_1, \ldots, A_n\rangle$ wynosi co najmniej $k(k-1)! = k!$ w pierwszym przypadku i $k(k-1)!/(k-n)! = k!/(k-n)!$ w drugim.

Przypadek 2: $|A_{i_1} \cup \ldots \cup A_{i_m}| = m$ dla pewnego ciągu $1 \leqslant i_1 < \ldots < i_m \leqslant n$, gdzie $1 \leqslant m \leqslant n-1$. Bez zmniejszenia ogólności możemy zakładać, iż $\{i_1, \ldots, i_m\} = \{1, \ldots, m\}$ (przy przenumerowaniu zbiorów A_i liczba systemów reprezentantów nie ulega zmianie). Mamy $k \leqslant m < n$, a więc na mocy założenia indukcyjnego istnieje co najmniej $k!$ systemów reprezentantów dla $\langle A_1, \ldots, A_m\rangle$. Wystarczy teraz wykazać, że ciąg $\langle A_{m+1} \setminus A, \ldots, A_n \setminus A\rangle$, gdzie $A = A_1 \cup \ldots \cup A_m$, ma system reprezentantów. Wtedy bowiem można rozszerzyć dowolny system reprezentantów dla $\langle A_1, \ldots, A_m\rangle$ do systemu reprezentantów dla $\langle A_1, \ldots, A_n\rangle$. Gdyby warunek Halla dla $\langle A_{m+1} \setminus A, \ldots, A_n \setminus A\rangle$ nie był spełniony, na przykład

$$|(A_{m+i_1} \setminus A) \cup \ldots \cup (A_{m+i_p} \setminus A)| < p \qquad (1 \leqslant i_i < \ldots < i_p \leqslant n,\ 1 \leqslant p \leqslant n-m),$$

to mielibyśmy

$$\begin{aligned} |A_1 \cup \ldots \cup A_m \cup A_{m+i_1} \cup \ldots \cup A_{m+i_p}| &= \\ &= |A_1 \cup \ldots \cup A_m \cup (A_{m+i_1} \setminus A) \cup \ldots \cup (A_{m+i_p} \setminus A)| = \\ &= |A_1 \cup \ldots \cup A_m| + |(A_{m+i_1} \setminus A) \cup \ldots \cup (A_{m+i_p} \setminus A)| < m+p, \end{aligned}$$

tzn. warunek Halla dla $\langle A_1, \ldots, A_n\rangle$ nie byłby spełniony, wbrew założeniom twierdzenia. Z założenia indukcyjnego (dla $k = 1$) wnioskujemy, że ciąg $\langle A_{m+1} \setminus A, \ldots, A_n \setminus A\rangle$ ma co najmniej jeden system reprezentantów. □

Zauważmy, że dowód twierdzenia 5.1 stanowi niezależny dowód twierdzenia Halla.

Z liczbą systemów reprezentantów związany jest problem wyznaczania tzw. permanentu macierzy. *Permanent* macierzy $A = [a_{ij}]$ o m wierszach, n kolumnach i elementach z dowolnego ciała definiujemy jako

$$\operatorname{per} A = \sum a_{1,\sigma(1)} a_{2,\sigma(2)} \ldots a_{m,\sigma(m)},$$

gdzie sumowanie rozciągnięte jest na wszystkie funkcje różnowartościowe $\sigma\colon \{1, \ldots, m\} \to \{1, \ldots, n\}$ (oczywiście $\operatorname{per} A = 0$ gdy $m > n$). Definicja permanentu przypomina bardzo definicję wyznacznika macierzy kwadratowej. Istotnie, dla $m = n$ sumujemy po wszystkich permutacjach zbioru $\{1, \ldots, m\}$, i jedyna różnica polega na tym, że w przypadku wyznacznika każdy ze składników

$a_{1,\sigma(1)}a_{2,\sigma(2)}\ldots a_{m,\sigma(m)}$ mnożymy przez 1 lub -1 w zależności od tego, czy σ jest permutacją parzystą czy nieparzystą. Wiele własności wyznacznika przenosi się na permanent (p. zad. 23–26, 29–31).

W rozdziale tym będziemy interesowali się głównie permanentem macierzy zero-jedynkowych, a powód tego jest następujący. Dowolnemu ciągowi $\langle A_1, \ldots, A_n\rangle$ podzbiorów zbioru $X = \{x_1, \ldots, x_m\}$ możemy przyporządkować jego macierz incydencji $A = [a_{ij}]$ o m wierszach i n kolumnach, gdzie $a_{ij} = 1$, jeśli $x_i \in A_j$, i $a_{ij} = 0$, jeśli $x_i \notin A_j$. Zachodzi następujące twierdzenie:

TWIERDZENIE 5.2. *Liczba systemów reprezentantów dla ciągu* $\langle A_1, \ldots, A_n\rangle$ *jest równa* per A^T, *gdzie* A *jest macierzą incydencji ciągu* $\langle A_1, \ldots, A_n\rangle$ (A^T *oznacza macierz transponowaną względem* A).

Dowód. Niech $A = [a_{ij}]$. Składnik $a_{\sigma(1)1}a_{\sigma(2),2}\ldots a_{\sigma(n),n}$ permanentu macierzy A^T jest równy jedności wtedy i tylko wtedy, gdy $x_{\sigma(1)} \in A_1, \ldots, x_{\sigma(n)} \in A_n$, tzn. gdy $x_{\sigma(1)}, \ldots, x_{\sigma(n)}$ jest systemem reprezentantów dla $\langle A_1, \ldots, A_n\rangle$. □

Zobaczmy teraz jak wygląda twierdzenie Halla w interpretacji macierzowej.

TWIERDZENIE 5.3 (Frobenius [1]). *Niech* A *będzie macierzą zero-jedynkową o* m *wierszach i* n *kolumnach* ($m \leqslant n$). *Permanent tej macierzy jest równy zeru wtedy i tylko wtedy, gdy zawiera ona podmacierz zerową wymiaru* $p\times r$, *gdzie* $p+r = n+1$.

Dowód. Rozważmy dowolny zbiór n-elementowy $X = \{x_1, \ldots, x_n\}$ oraz niech $\langle A_1, \ldots, A_m\rangle$ będzie ciągiem jego podzbiorów takim, że $x_j \in A_i \Leftrightarrow a_{ij} = 1$ ($1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$). Z twierdzenia Halla i twierdzenia 5.2 wnioskujemy, że per $A = 0$ wtedy i tylko wtedy, gdy nie jest spełniony warunek Halla dla $\langle A_1, \ldots, A_m\rangle$. Z kolei niespełnienie warunku Halla jest równoważne istnieniu pewnego podzbioru k wierszy macierzy A takich, że wszystkie jedynki w tych wierszach można pokryć $k-1$ kolumnami. Podmacierz wymiaru $k\times(n-k+1)$ określona przez te k wierszy i pozostałe $n-(k-1)$ kolumn składa się oczywiście z samych zer, a $k+n-(k-1) = n+1$. Na odwrót, jeśli podmacierz wyznaczona przez pewne p wierszy i r kolumn ($p+r = n+1$) składa się z samych zer, to jedynki w tych p wierszach można pokryć $n-r = n-(n+1-p) = p-1$ kolumnami. Oznacza to, że warunek Halla dla $\langle A_1, \ldots, A_n\rangle$ nie jest spełniony, a więc, na mocy twierdzenia Halla i twierdzenia 5.2, per $A = 0$. □

Warto wspomnieć, że powyższe twierdzenie zostało opublikowane przez Frobeniusa w roku 1912, a więc znacznie wcześniej niż praca P. Halla (1935). Jest ono oczywiście prawdziwe dla dowolnych macierzy o elementach rzeczywistych nieujemnych.

Jeszcze prościej można udowodnić twierdzenie Frobeniusa korzystając z twierdzenia węgierskiego. Wystarczy w tym celu zauważyć, że per $A = 0$ wtedy i tylko wtedy, gdy w A nie ma zbioru rozproszonego jedynek o liczności m, oraz że jeśli jedynki w A można pokryć p wierszami i q kolumnami, to pozostałe wiersze i kolumny wyznaczają podmacierz wymiaru $(m-p)\times(n-q)$ złożoną z samych zer

Zauważmy, że dodanie do kolumny (wiersza) kombinacji liniowej pozostałych kolumn (wierszy) zmienia na ogół wartość permanentu (w przeciwieństwie do wyznacznika macierzy kwadratowej). Powoduje to, iż obliczanie permanentu jest na ogół trudniejsze niż obliczanie wyznacznika. Jedną z możliwych metod jest korzystanie z odpowiednika rozwinięcia Laplace'a (p. zad. 26). Inną możliwość daje następujące twierdzenie:

TWIERDZENIE 5.4. *Niech A będzie macierzą zero-jedynkową o m wierszach i n kolumnach* ($m \leqslant n$). *Oznaczmy*

$$S_r(A) = \sum S(A_{i_1 \dots i_r}),$$

gdzie sumowanie rozciąga się na wszystkie ciągi $1 \leqslant i_1 < \dots < i_r \leqslant n$, $A_{i_1 \dots i_r}$ *oznacza macierz powstałą z A przez zastąpienie zerami elementów kolumn o numerach* $i_1, \dots, i_r$, $S(A_{i_1 \dots i_r})$ *zaś oznacza iloczyn sum wierszy macierzy* $A_{i_1 \dots i_r}$. *Wówczas*

$$\operatorname{per} A = S_{n-m}(A) - \binom{n-m+1}{1} S_{n-m+1}(A) + \binom{n-m+2}{2} S_{n-m+2}(A) - \dots +$$
$$+ (-1)^{m-1} \binom{n-1}{m-1} S_{n-1}(A).$$

Dowód. Niech $A = [a_{ij}]$ i niech X będzie zbiorem wszystkich ciągów $\langle j_1, \dots, j_m \rangle$ takich, że $1 \leqslant j_1 \leqslant n, \dots, 1 \leqslant j_m \leqslant n$ oraz $a_{1,j_1} = \dots = a_{m,j_m} = 1$. Niech P_i będzie zbiorem tych ciągów z X, które nie zawierają i ($1 \leqslant i \leqslant n$). Łatwo zauważyć, że liczność zbioru $P_{i_1} \cap \dots \cap P_{i_r}$, tzn. liczba tych ciągów z X, które nie zawierają $i_1, \dots, i_r$ (i być może pewnych innych liczb) jest równa $S(A_{i_1, \dots, i_r})$. Istotnie,

$$\prod_{i=1}^{m} \sum_{j=1}^{n} a_{ij} = \sum_{1 \leqslant j_1 \leqslant n, \dots, 1 \leqslant j_m \leqslant n} a_{1,j_1} \dots a_{m,j_m}.$$

Zauważmy, że per A jest równy liczbie tych ciągów $\langle j_1, \dots, j_m \rangle \in X$, w których występuje dokładnie m liczb, tzn. które nie zawierają dokładnie $n-m$ liczb. Na mocy zasady włączania–wyłączania (rozdz. 1, wniosek 7.2) mamy zatem

$$\operatorname{per} A = \sum_{1 \leqslant i_1 < \dots < i_{n-m} \leqslant n} S(A_{i_1 \dots i_{n-m}}) - \binom{n-m+1}{1} \sum_{1 \leqslant i_1 < \dots < i_{n-m+1} \leqslant n} S(A_{i_1 \dots i_{n-m+1}}) +$$
$$+ \dots + (-1)^{m-1} \binom{n-1}{m-1} \sum_{1 \leqslant i_1 < \dots < i_{n-1} \leqslant n} S(A_{i_1 \dots i_{n-1}}),$$

co jest jedynie innym zapisem równości, którą mieliśmy udowodnić. □

Szczególnie prosty wzór otrzymujemy w przypadku macierzy kwadratowych:

WNIOSEK 5.5. *Jeśli A jest macierzą zero-jedynkową wymiaru* $n \times n$, *to*

$$\operatorname{per} A = S(A) - S_1(A) + S_2(A) - \dots + (-1)^{n-1} S_{n-1}(A). \ \square$$

Na zakończenie tego paragrafu warto odnotować następujący fakt, z którego niejednokrotnie już korzystaliśmy w tym rozdziale. Otóż wiele dotychczas podanych twierdzeń może być sformułowanych równoważnie dla każdego z czterech poniżej wymienionych obiektów:

(1) Ciąg $\langle A_1, \ldots, A_n \rangle$ podzbiorów zbioru $\{x_1, \ldots, x_m\}$.

(2) Macierz zero-jedynkowa $[a_{ij}]$ wymiaru $m \times n$ $(a_{ij} = 1 \Leftrightarrow x_i \in A_j)$.

(3) Graf dwudzielny o zbiorze wierzchołków $\{x_1, \ldots, x_m\} \cup \{y_1, \ldots, y_n\}$ ($\{x_i, y_j\}$ jest krawędzią wtedy i tylko wtedy, gdy $x_i \in A_j$).

(4) Zbiór częściowo uporządkowany $\langle P, \leqslant \rangle$, gdzie $P = \{x_1, \ldots, x_m\} \cup \cup \{y_1, \ldots, y_n\}$ ($x < y$ wtedy i tylko wtedy, gdy $x = x_i$, $y = y_j$ i $x_i \in A_j$).

Mając dane twierdzenie w jednym sformułowaniu można otrzymać zupełnie mechanicznie nowe twierdzenie przechodząc do innego sformułowania. Szczególnie ciekawe może być przejście z (3) (lub (2)) — gdzie rola zbiorów $\{x_1, \ldots, x_m\}$ i $\{y_1, \ldots, y_n\}$ jest symetryczna — do (1). Otrzymujemy wtedy z jednego twierdzenia dotyczącego grafów dwudzielnych dwa formalnie różne twierdzenia o systemach reprezentantów.

§ 6. Macierze bistochastyczne

Podamy najpierw kilka definicji pomocniczych. Macierz zero-jedynkową $[a_{ij}]$ wymiaru $n \times n$ nazywamy *macierzą permutacyjną*, jeśli każda linia (tzn. wiersz lub kolumna) tej macierzy zawiera dokładnie jedną jedynkę, innymi słowy, jeśli dla pewnej permutacji π zbioru $\{1, \ldots, n\}$ mamy $a_{i,\pi(i)} = 1$ oraz $a_{ij} = 0$ dla $j \neq \pi(i)$ $(1 \leqslant i, j \leqslant n)$. Macierze permutacyjne są szczególnym przypadkiem *macierzy bistochastycznych*, tzn. macierzy o elementach rzeczywistych nieujemnych, o sumie elementów w każdej linii równej jedności. Oczywiście każda macierz bistochastyczna jest kwadratowa (wystarczy policzyć sumę elementów w całej macierzy na dwa sposoby: „wierszami" i „kolumnami"). Łatwo sprawdzić, że każda wypukła kombinacja $\mu_1 A_1 + \ldots + \mu_k A_k$ $(\mu_1 + \ldots + \mu_k = 1,\ \mu_1, \ldots, \mu_k \geqslant 0)$ macierzy permutacyjnych $A_1, \ldots, A_k$ jest macierzą bistochastyczną. Głównym wynikiem tego paragrafu będzie fakt, że zachodzi również twierdzenie odwrotne:

TWIERDZENIE 6.1 (Birkhoff [1]). *Każda macierz bistochastyczna jest kombinacją wypukłą macierzy permutacyjnych.*

Dowód. Niech $A = [a_{ij}]$ będzie macierzą bistochastyczną wymiaru $n \times n$. Wykażemy najpierw, że $a_{1,\pi(1)}, \ldots, a_{n,\pi(n)} > 0$ dla pewnej permutacji π. Wystarczy w tym celu udowodnić, że per $A \neq 0$. Przypuśćmy, że per $A = 0$. Na mocy twierdzenia Frobeniusa istnieje wtedy podzbiór p wierszy oraz podzbiór r kolumn $(p+r = n+1)$ o tej własności, że wszystkie elementy podmacierzy wymiaru $p \times r$ wyznaczonej przez te wiersze i kolumny są równe zeru. Wobec $p+r > n$ mamy $n-r < p$. Dochodzimy do sprzeczności: z jednej strony suma elementów w

naszych p wierszach jest równa p, z drugiej zaś strony (licząc „kolumnami") jest nie większa niż $n-r < p$.

Tak więc $a_{1,\pi(1)}, \ldots, a_{n,\pi(n)} > 0$ dla pewnej permutacji π. Niech ε będzie najmniejszą z liczb $a_{1,\pi(1)}, \ldots, a_{n,\pi(n)}$ oraz niech $P = [p_{ij}]$ będzie macierzą permutacyjną odpowiadającą permutacji π (tzn. $p_{ij} = 1 \Leftrightarrow j = \pi(i)$). Suma elementów każdej linii macierzy $A - \varepsilon P$ jest równa $1-\varepsilon$, zatem macierz $B = (1-\varepsilon)^{-1}(A-\varepsilon P)$ jest bistochastyczna. Otrzymujemy stąd równość

$$A = \varepsilon P + (1-\varepsilon) B,$$

gdzie B jest macierzą bistochastyczną, w której liczba niezerowych elementów jest co najmniej o jeden mniejsza niż w A, w B mamy bowiem zero w pozycji, w której w A występował element $a_{i,\pi(i)} = \varepsilon$. Twierdzenie nasze wynika przez indukcję względem liczby niezerowych elementów w A: Załóżmy, że w A mamy m niezerowych elementów, i że dla dowolnych macierzy B o mniej niż m niezerowych elementach twierdzenie jest prawdziwe. Mamy wtedy

$$A = \varepsilon P + (1-\varepsilon) B = \varepsilon P + (1-\varepsilon)(\mu_1 P_1 + \ldots + \mu_k P_k) =$$
$$= \varepsilon P + (1-\varepsilon)\mu_1 P_1 + \ldots + (1-\varepsilon)\mu_k P_k,$$

gdzie $\sum_i \varepsilon_i P_i$ jest rozkładem macierzy B na kombinację wypukłą macierzy permutacyjnych, który istnieje na mocy założenia indukcyjnego. □

Na twierdzenie Birkhoffa można spojrzeć nieco inaczej. Zbiór $\mathcal{D}_n$ wszystkich macierzy bistochastycznych wymiaru $n \times n$ możemy traktować jako podzbiór n^2-wymiarowej przestrzeni euklidesowej. Można łatwo sprawdzić, że zbiór $\mathcal{D}_n$ jest domkniętym, ograniczonym, wypukłym podzbiorem tej przestrzeni, zaś punkty ekstremalne tego zbioru to dokładnie macierze permutacyjne (punkt x zbioru wypukłego W jest *ekstremalny*, jeśli nie jest postaci $\alpha y + (1-\alpha) z$, gdzie $0 < \alpha < 1$, $y, z \in W$, $y \neq z$). W tych terminach twierdzenie Birkhoffa jest szczególnym przypadkiem ogólniejszego twierdzenia, które orzeka, iż dowolny domknięty, ograniczony, wypukły podzbiór przestrzeni euklidesowej jest otoczką wypukłą swoich punktów ekstremalnych (*otoczka wypukła* dowolnego zbioru A jest to najmniejszy zbiór wypukły $B \supseteq A$; można łatwo wykazać, że pokrywa się ona ze zbiorem wszystkich kombinacji wypukłych elementów zbioru A).

Stosując dokładnie taką samą metodę jak w dowodzie twierdzenia 6.1 możemy udowodnić następujący fakt:

TWIERDZENIE 6.2. *Niech A będzie macierzą zero-jedynkową o sumie elementów w każdej linii równej k. Wówczas $A = P_1 + \ldots + P_k$, gdzie $P_1, \ldots, P_k$ są macierzami permutacyjnymi.*

W § 7 udowodnimy pewne uogólnienie tego twierdzenia (p. lemat 7.3).

§ 7. Zastosowania do kwadratów łacińskich

Prostokątem łacińskim typu $\langle r, s, n\rangle$ nazywamy macierz wymiaru $r\times s$ o elementach ze zbioru $\{1, \ldots, n\}$, której żadna linia nie zawiera dwóch takich samych elementów. Prostokąt łaciński typu $\langle n, n, n\rangle$ nazywamy *kwadratem łacińskim rzędu n*. Oczywiście każda linia kwadratu łacińskiego rzędu n zawiera liczby $1, \ldots, n$ w pewnej kolejności. Korzystając z twierdzenia Halla o liczbie systemów reprezentantów podamy teraz pewne oszacowanie dolne na liczbę kwadratów łacińskich rzędu n. Będziemy mówili, że prostokąt łaciński R^* typu $\langle r^*, s^*, m^*\rangle$ jest *rozszerzeniem* prostokąta łacińskiego R typu $\langle r, s, m\rangle$, jeśli R jest podmacierzą wyznaczoną przez r pierwszych wierszy i s pierwszych kolumn macierzy R^*.

TWIERDZENIE 7.1 (M. Hall). *Niech* $0 < r < n$. *Dowolny prostokąt łaciński* R *typu* $\langle r, n, n\rangle$ *można rozszerzyć na co najmniej* $(n-r)!$ *sposobów do prostokąta łacińskiego* R^* *typu* $\langle r+1, n, n\rangle$.

Dowód. Rozważmy ciąg $\langle A_1, \ldots, A_n\rangle$, gdzie A_i jest zbiorem tych liczb spośród $1, \ldots, n$, które nie występują w i-tej kolumnie macierzy R. Mamy oczywiście $|A_1| = \ldots = |A_n| = n-r$. Każda z liczb $i\in\{1, \ldots, n\}$ występuje w R dokładnie r razy (raz w każdym wierszu). W jednej kolumnie może być co najwyżej jedno takie wystąpienie, zatem i występuje dokładnie w $n-r$ spośród zbiorów $A_1, \ldots, A_n$. Niech $1\leqslant k < n$ i niech $1 \leqslant i_1 < \ldots < i_k \leqslant n$. Załóżmy, że suma $A_{i_1}\cup\ldots\cup A_{i_k}$ zawiera p elementów, powiedzmy $A_{i_1}\cup\ldots\cup A_{i_k} = \{x_1, \ldots, x_p\}$. Obliczmy na dwa sposoby liczbę wystąpień elementów $x_1, \ldots, x_p$ w zbiorach $A_{i_1}, \ldots, A_{i_k}$, tzn. liczbę par $\langle x_j, A_{i_m}\rangle$ takich, że $x_j\in A_{i_m}$, $1\leqslant j\leqslant p$, $1\leqslant m\leqslant k$. Z jednej strony liczba ta jest równa $k(n-r)$ (każdy bowiem ze zbiorów $A_{i_1}, \ldots, A_{i_k}$ zawiera $n-r$ elementów), z drugiej zaś strony liczba ta jest nie większa niż $p(n-r)$ (gdyż każdy spośród elementów $x_1, \ldots, x_p$ występuje w $n-r$ spośród zbiorów $A_1, \ldots, A_n$, a więc w nie więcej niż $n-r$ spośród zbiorów $A_{i_1}, \ldots, A_{i_k}$). Mamy stąd $k(n-r)\leqslant p(n-r)$, czyli $k\leqslant p$. Oznacza to, że dla ciągu $\langle A_1, \ldots, A_n\rangle$ spełniony jest warunek Halla. Na mocy twierdzenia 5.1 istnieje dla niego co najmniej $(n-r)!$ systemów reprezentantów. Nasze twierdzenie wynika teraz z faktu, iż jeśli dołączymy do R dowolny taki system reprezentantów jako nowy wiersz, to otrzymamy prostokąt łaciński typu $\langle r+1, n, n\rangle$. □

Otrzymujemy stąd następujący

WNIOSEK 7.2. *Istnieje co najmniej*

$$n!(n-1)!\ldots(n-r+1)!$$

prostokątów łacińskich typu $\langle r, n, n\rangle$, *w szczególności co najmniej*

$$n!(n-1)!\ldots 1!$$

kwadratów łacińskich rzędu n.

Dowód. Twierdzenie wynika przez indukcję względem r z twierdzenia 7.1 oraz z oczywistego faktu, że istnieje dokładnie $n!$ prostokątów łacińskich typu $\langle 1, n, n\rangle$. Istotnie, mając $n!(n-1)!\ldots(n-(r-1)+1)!$ prostokątów łacińskich typu $\langle r-1, n, n\rangle$ możemy każdy z nich rozszerzyć na $(n-(r-1))!$ sposobów otrzymując w sumie $n!(n-1)!\ldots(n-r+1)!$ prostokątów łacińskich typu $\langle r, n, n\rangle$. □

Oszacowanie podane we wniosku 7.2 jest bardzo niedokładne. Jeśli przez l_n oznaczymy liczbę *znormalizowanych* kwadratów łacińskich rzędu n, tzn. kwadratów, w których elementy zarówno pierwszego wiersza jak i pierwszej kolumny występują w naturalnym porządku $1, 2, \ldots, n$, to z wniosku 7.2 wynika, że $l_n \geqslant (n-2)!(n-3)!\ldots 1!$ (iloczyn ten interpretujemy jako 1 dla $n \leqslant 2$). Istotnie, łatwo zauważyć, że każdemu kwadratowi znormalizowanemu odpowiada $n!(n-1)!$ kwadratów powstałych przez dokonanie najpierw dowolnej permutacji kolumn, a następnie dowolnej permutacji wierszy o numerach $2, 3, \ldots, n$. Oto porównanie kilku znanych wartości l_n z $b_n = (n-2)!\ldots 1!$:

Rząd kwadratu łacińskiego	l_n	b_n	liczba klas izotopii
1	1	1	1
2	1	1	1
3	1	1	1
4	4	2	2
5	56	12	2
6	9 408	288	22
7	16 942 080	34 560	563
8	535 281 401 856	1 393 459 200	1 676 257
9	377 597 570 964 258 816	505 658 474 496 000	?

Przy okazji w tablicy podano liczbę „istotnie różnych" kwadratów łacińskich. Dokładniej, będziemy mówili, że kwadraty $L_1 = [a_{ij}]$, $L_2 = [b_{ij}]$ są *izotopijne*, jeśli L_2 powstaje z L_1 przez dokonanie pewnej permutacji wierszy, pewnej permutacji kolumn i pewnej permutacji symboli występujących w L_1 (symboli, a nie ich wystąpień!), tzn. jeśli $\vartheta(a_{ij}) = b_{\varphi(i),\psi(j)}$, dla pewnych permutacji φ, ψ, ϑ zbioru $\{1, \ldots, n\}$ (n jest rzędem L_1 i L_2). Łatwo sprawdzić, że relacja izotopii jest relacją równoważności. W tablicy podano liczbę klas tej relacji, na jaką rozpada się zbiór wszystkich kwadratów łacińskich rzędu n.

Dotychczas zajmowaliśmy się rozszerzaniem prostokąta łacińskiego typu $\langle r, s, n\rangle$ do kwadratu łacińskiego rzędu n jedynie w przypadku $s = n$. W ogólnym przypadku rozszerzenie takie nie zawsze jest możliwe. Na przykład prostokąt łaciński typu $\langle 2, 2, 3\rangle$

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$$

nie daje się rozszerzyć do kwadratu łacińskiego rzędu 3. Do dowodu twierdzenia dającego pełną charakteryzację „rozszerzalnych" prostokątów łacińskich potrzebny nam będzie pewien lemat będący uogólnieniem twierdzenia 6.2. Przez *uogólnioną macierz permutacyjną* będziemy rozumieli dowolną macierz zero-jedynkową wymiaru $m \times n$, w której suma elementów każdego wiersza równa jest 1, a suma elementów dowolnej kolumny jest nie większa niż 1 (oczywiście musi być $m \leqslant n$).

LEMAT 7.3. *Niech A będzie macierzą zero-jedynkową wymiaru $m \times n$, gdzie $m \leqslant n$, o sumie elementów każdego wiersza równej k i sumie elementów i-tej kolumny równej s_i, gdzie*

$$k-(n-m) \leqslant s_i \leqslant k \quad (1 \leqslant i \leqslant n).$$

Wówczas $A = P_1 + \ldots + P_k$, gdzie $P_1, \ldots, P_k$ są uogólnionymi macierzami permutacyjnymi.

Dowód. Wykażemy najpierw, że jeśli $m < n$, to macierz naszą można rozszerzyć przez dodanie $n-m$ wierszy tak, by otrzymana macierz $\bar{A}$ wymiaru $n \times n$ miała dokładnie k jedynek w każdej linii. Niech p będzie liczbą kolumn macierzy A zawierających $k-(n-m)$ jedynek, q zaś liczbą kolumn zawierających mniej niż k jedynek (zakładamy $m < n$). Szacując liczbę jedynek w macierzy A otrzymujemy:

$$mk \leqslant p(k-n+m)+(n-p)k, \qquad mk \leqslant pk-pn+pm+nk-pk,$$
$$(n-m)p \leqslant (n-m)k, \qquad p \leqslant k$$

oraz

$$mk \geqslant (n-q)k+q(k-n+m), \qquad mk \geqslant nk-qk+qk-qn+qm,$$
$$(n-m)q \geqslant (n-m)k, \qquad q \geqslant k.$$

Tak więc $p \leqslant k \leqslant q$, i do macierzy A możemy dodać $(m+1)$-szy wiersz zawierający k jedynek taki, że jedynki występują tylko w kolumnach dla których $s_i < k$, przy czym we wszystkich kolumnach, dla których $s_i = k-(n-m)$. Otrzymujemy w ten sposób macierz A wymiaru $(m+1) \times n$, w której suma s_i^* elementów i-tej kolumny spełnia nierówność $k-\big(n-(m+1)\big) \leqslant s_i^* \leqslant k$ dla $1 \leqslant i \leqslant n$. Powtarzając tę konstrukcję otrzymujemy ostatecznie macierz $\bar{A}$ wymiaru $n \times n$, w której suma $\bar{s}_i$ elementów i-tej kolumny spełnia nierówność $k-(n-n) \leqslant \bar{s}_i \leqslant k$, tzn. każda linia macierzy $\bar{A}$ zawiera k jedynek. Na mocy twierdzenia 5.2 $\bar{A} = \bar{P}_1 + \ldots + \bar{P}_k$, gdzie $\bar{P}_1, \ldots, \bar{P}_k$ są macierzami permutacyjnymi. Żądany rozkład $A = P_1 + \ldots + P_k$ na sumę uogólnionych macierzy permutacyjnych otrzymujemy przyjmując jako P_i podmacierz złożoną z pierwszych m wierszy macierzy $\bar{P}_i$ $(1 \leqslant i \leqslant k)$. □

A oto zapowiedziana charakteryzacja rozszerzalnych prostokątów łacińskich:

TWIERDZENIE 7.4 (Ryser [1]). *Niech R będzie prostokątem łacińskim typu $\langle r, s, n\rangle$ i niech $N(i)$ oznacza liczbę wystąpień elementu i w tym prostokącie*

$(1 \leqslant i \leqslant n)$. *Prostokąt R może być rozszerzony do kwadratu łacińskiego rzędu n wtedy i tylko wtedy, gdy*

$$N(i) \geqslant r+s-n$$

dla $1 \leqslant i \leqslant n$,

Dowód. Konieczność warunku jest prosta. Jeśli prostokąt R daje się rozszerzyć do pewnego kwadratu L rzędu n, to pierwszych r wierszy tego kwadratu zawiera dokładnie r wystąpień liczby i. Lecz i nie może występować więcej niż $n-s$ razy w $n-s$ nowych kolumnach dodanych do R. Tak więc i musi występować w R co najmniej $r-(n-s) = r+s-n$ razy.

Dla dowodu dostateczności załóżmy, że $N(i) \geqslant r+s-n$ dla $1 \leqslant i \leqslant n$. Niech A_i będzie zbiorem tych liczb spośród $1, \ldots, n$, które nie występują w i-tym wierszu prostokąta R $(1 \leqslant i \leqslant r)$. Utwórzmy macierz zero-jedynkową $A = [a_{ij}]$ wymiaru $r \times n$, gdzie $a_{ij} = 1 \Leftrightarrow j \in A_i$. Suma każdego wiersza macierzy A jest równa $n-s$ (gdyż $|A_i| = n-s$ dla $1 \leqslant i \leqslant r$), suma zaś j-tej kolumny równa jest $r-N(j)$ dla $1 \leqslant j \leqslant n$. Wobec nierówności $N(j) \geqslant r+s-n$ mamy

$$r-N(j) \leqslant n-s.$$

Z drugiej strony, wobec $N(j) \leqslant s$, otrzymujemy

$$(n-s)-(n-r) = r-s \leqslant r-N(j).$$

Tak więc $(n-s)-(n-r) \leqslant r-N(j) \leqslant n-s$, i na mocy lematu 7.3 $A = P_1 + \ldots + P_{n-s}$, gdzie $P_1, \ldots, P_{n-s}$ są uogólnionymi macierzami permutacyjnymi. Każda z tych macierzy określa nową kolumnę, którą dodajemy do prostokąta R, w następujący sposób: Jeśli w macierzy $P_k = [p_{ij}]$ $(1 \leqslant k \leqslant n-s)$ mamy $p_{1,i_1} = \ldots = p_{r,i_r} = 1$, to k-ta spośród nowych kolumn zawiera liczby $i_1, \ldots, i_r$ (i_j w j-tym wierszu, $1 \leqslant j \leqslant r$).

Otrzymany w ten sposób prostokąt łaciński typu $\langle r, n, n\rangle$ można – na mocy twierdzenia 7.1 – rozszerzyć do kwadratu łacińskiego rzędu n. □

Do zagadnień związanych z kwadratami łacińskimi powrócimy jeszcze w rozdziale 7 (§ 9). Czytelnikowi pragnącemu głębiej poznać ten dział kombinatoryki polecamy obszerną monografię Dénesa i Keedwella [1].

§ 8. Selektory, selektory częściowe i twierdzenie Edmondsa–Fulkersona

Ściśle związane z pojęciem systemu reprezentantów jest pojęcie selektora. Jeśli $\langle x_1, \ldots, x_n\rangle$ jest systemem reprezentantów dla ciągu $\langle A_1, \ldots, A_n\rangle$, to mówimy, że zbiór $\{x_1, \ldots, x_n\}$ jest *selektorem ciągu* $\langle A_1, \ldots, A_n\rangle$. Innymi słowy, zbiór S jest selektorem ciągu $\langle A_1, \ldots, A_n\rangle$, jeśli dla pewnego wzajemnie jednoznacznego odwzorowania φ: $S \to \{1, \ldots, n\}$ mamy $x \in A_{\varphi(x)}$ dla każdego $x \in S$. Oczywiście,

zbiór S jest selektorem dla $\langle A_1, \ldots, A_n\rangle$ wtedy i tylko wtedy, gdy jest selektorem ciągu $A_{\sigma(1)}, \ldots, A_{\sigma(n)}$ dla każdej permutacji σ. Możemy więc mówić o selektorze rodziny $(A_1, \ldots, A_n)$: zbiór S jest *selektorem rodziny* $(A_1, \ldots, A_n)$, jeśli jest selektorem ciągu $\langle A_1, \ldots, A_n\rangle$. Ciąg zbiorów ma system reprezentantów wtedy i tylko wtedy, gdy ma selektor, warunek Halla jest więc warunkiem koniecznym i dostatecznym istnienia selektora. Jednakże liczba selektorów jest na ogół znacznie mniejsza od liczby systemów reprezentantów. Na przykład ciąg $\langle A_1, \ldots, A_n\rangle$, gdzie $A_1 = \ldots = A_n = \{1, \ldots, n\}$ ma $n!$ systemów reprezentantów, lecz tylko jeden selektor.

W przypadku, gdy nie istnieje selektor, naturalne staje się pytanie „jak dużo brakuje do jego istnienia". W tym kontekście pożyteczne jest pojęcie selektora częściowego. Będziemy mówili, że zbiór S jest *selektorem częściowym* ciągu $\langle A_1, \ldots, A_n\rangle$ (rodziny $(A_1, \ldots, A_n)$), jeśli S jest selektorem pewnego podciągu ciągu $\langle A_1, \ldots, A_n\rangle$ (pewnej podrodziny rodziny $(A_1, \ldots, A_n)$), tzn. jeśli istnieje funkcja różnowartościowa $\varphi\colon S \to \{1, \ldots, n\}$ taka, że $x \in A_{\varphi(x)}$ dla każdego $x \in S$. Oczywiście, dowolny podzbiór selektora częściowego jest również selektorem częściowym (zbiór pusty uważamy również za selektor częściowy). Liczbę $n-|S|$ nazywamy *defektem selektora częściowego* S. Okazuje się, że nieformalna odpowiedź na nasze nieformalne pytanie jest następująca: „do istnienia selektora brakuje dokładnie tyle, ile brakuje do spełnienia warunku Halla". Dokładniej wyraża to następujące twierdzenie.

TWIERDZENIE 8.1 (Hall i Ore, por. Ore [1]). *Ciąg $\langle A_1, \ldots, A_n\rangle$ ma selektor częściowy o defekcie d wtedy i tylko wtedy, gdy dla każdego $J \subseteq \{1, \ldots, n\}$*

$$\Big|\bigcup_{j\in J} A_j\Big| \geqslant |J| - d. \tag{8.1}$$

Dowód. Utwórzmy zbiór częściowo uporządkowany $\langle X, \leqslant\rangle$ o $m+n$ elementach $x_1, \ldots, x_m, y_1, \ldots, y_n$, gdzie $\{x_1, \ldots, x_m\} = \bigcup_{i=1}^{n} A_n$, przyjmując, że $z < t$ wtedy i tylko wtedy, gdy $z = x_i$, $t = y_j$, $x_i \in A_j$ dla pewnych i, j $(1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n)$. Niech

$$\{x_{i_1}, \ldots, x_{i_k}, y_{j_1}, \ldots, y_{j_h}\}$$

będzie antyłańcuchem o maksymalnej liczności. Mamy wtedy

$$A_{j_1} \cup \ldots \cup A_{j_h} \subseteq \{x_1, \ldots, x_m\} \setminus \{x_{i_1}, \ldots, x_{i_h}\}. \tag{8.2}$$

Jeśli warunek (8.1) jest spełniony, to z (8.1) i (8.2) otrzymujemy $h-d \leqslant$ $\leqslant |A_{j_1} \cup \ldots \cup A_{j_h}| \leqslant m-k$, a stąd

$$k+h \leqslant m+d. \tag{8.3}$$

Skoro $s = k+h$ jest maksymalną licznością antyłańcucha w $\langle X, \leqslant\rangle$, możemy — na mocy twierdzenia Dilwortha — rozłożyć X na sumę s łańcuchów parami

rozłącznych. Zauważmy, że każdy łańcuch w $\langle X, \leqslant \rangle$ zawiera co najwyżej dwa elementy. Nasz rozkład ma więc postać

(8.4) $$X = \{x_{k_1}, y_{l_1}\} \cup \ldots \cup \{x_{k_p}, y_{l_p}\} \cup \{z_1\} \cup \ldots \cup \{z_q\},$$

gdzie $p+q = s$. Suma naszych s łańcuchów zawiera $m+n$ elementów zbioru X, stąd $2p+q = m+n$, czyli $p = m+n-(p+q) = m+n-s$. Wobec (8.3) $p \geqslant m+n-(m+d) = n-d$. Lecz $x_{k_1} \in A_{l_1}, \ldots, x_{k_p} \in A_{l_p}$, co oznacza, że zbiór $\{x_{k_1}, \ldots, x_{k_p}\}$ jest selektorem częściowym o defekcie $n-p \leqslant d$.

Na odwrót, jeśli $S = \{x_{i_1}, \ldots, x_{i_{n-d}}\}$ jest selektorem częściowym o defekcie d, to suma k spośród zbiorów $A_1, \ldots, A_n$ zawiera co najmniej $k-d$ elementów tego selektora. Warunek (8.1) jest więc konieczny. □

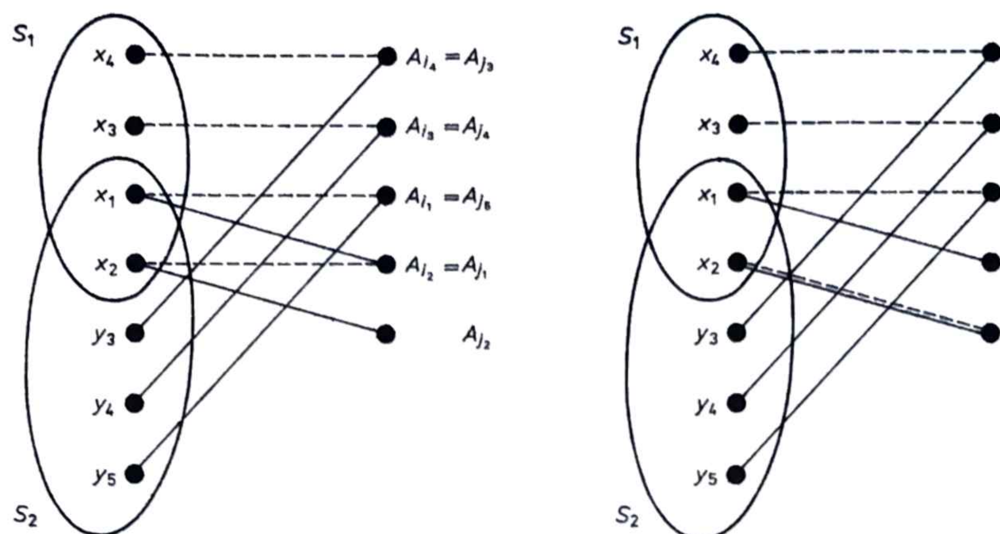
Twierdzenie Halla–Ore można również łatwo udowodnić przez sprowadzenie do twierdzenia Halla. Przytoczyliśmy tu jednak inny dowód, aby pokazać jeszcze jeden niezależny dowód twierdzenia Halla. Zauważmy, że w dowodzie tym, podobnie jak i w dowodzie twierdzenia węgierskiego (tw. 1.6) korzystaliśmy z twierdzenia Dilwortha jedynie dla zbiorów częściowo uporządkowanych o bardzo prostej strukturze. Dlatego też twierdzenie Dilwortha wydaje się być najbardziej głębokim spośród twierdzeń minimaksowych tego rozdziału (twierdzeniu Halla–Ore można również nadać postać minimaksową: Minimalny defekt selektora jest równy maksymalnej wartości wyrażenia $|J| - |\bigcup_{j \in J} A_j|$ dla $J \subseteq \{1, \ldots, n\}$).

Na zakończenie tego paragrafu udowodnimy jeszcze jedno ważne twierdzenie dotyczące selektorów częściowych pochodzące od Edmondsa i Fulkersona.

Twierdzenie 8.2 (Edmonds i Fulkerson [1]). *Niech S_1 i S_2 będą dwoma selektorami częściowymi ciągu $\langle A_1, \ldots, A_n \rangle$ i niech $|S_2| = |S_1|+1$. Wówczas istnieje element $y \in S_2 \setminus S_1$ taki, że $S_1 \cup \{y\}$ jest selektorem częściowym ciągu $\langle A_1, \ldots, A_n \rangle$.*

Dowód (Mirsky i Perfect [1]). Możemy zakładać, że $S_1 = \{x_1, \ldots, x_p\}$, $S_2 = \{y_1, \ldots, y_{p+1}\}$, gdzie $x_i = y_i$ dla $1 \leqslant i \leqslant r = |S_1 \cap S_2|$. Jeśli $r = p$ (tzn. $S_1 \subseteq S_2$), to twierdzenie jest oczywiście prawdziwe. Niech więc $r < p$, i załóżmy, że $\langle x_1, \ldots, x_p \rangle$ jest systemem reprezentantów dla $\langle A_{i_1}, \ldots, A_{i_p} \rangle$, zaś $\langle y_1, \ldots, y_{p+1} \rangle$ jest systemem reprezentantów dla $\langle A_{j_1}, \ldots, A_{j_{p+1}} \rangle$ (wskaźniki $i_1, \ldots, i_p$ są parami różne, podobnie jak $j_1, \ldots, j_{p+1}$). Rozpatrzmy następującą konstrukcję, która albo znajduje element y, o którym mowa w tezie twierdzenia, albo zastępuje ciąg $\langle A_{i_1}, \ldots, A_{i_p} \rangle$ pewnym nowym ciągiem, dla którego $\langle x_1, \ldots, x_p \rangle$ jest również systemem reprezentantów (p. rys. 21).

Konstrukcja. Nie może być $\{j_1, \ldots, j_{p+1}\} \subseteq \{i_1, \ldots, i_p\}$, a zatem $j_h \notin \{i_1, \ldots, i_p\}$ dla pewnego $h \leqslant p+1$. Jeśli wskaźnik h może być tak wybrany, by $r+1 \leqslant h \leqslant p+1$, to $\langle x_1, \ldots, x_p, y_h \rangle$ jest systemem reprezentantów dla $\langle A_{i_1}, \ldots, A_{i_p}, A_{j_h} \rangle$ a więc $S_1 \cup \{y_h\}$ jest żądanym selektorem częściowym ciągu $\langle A_1, \ldots, A_n \rangle$ W przeciwnym przypadku, tzn. gdy $1 \leqslant h \leqslant r$, mamy $x_h = y_h$ i ciąg $\langle x_1, \ldots, x_p \rangle$ jest systemem reprezentantów dla $\langle A_{i_1}, \ldots, A_{i_{h-1}}, A_{j_h}, A_{i_{h+1}}, \ldots, A_{i_p} \rangle$ (koniec konstrukcji).



Rys. 21. Do dowodu twierdzenia Edmondsa–Fulkersona

Przyjrzyjmy się bliżej temu ostatniemu ciągowi, a szczególnie jego pierwszym r pozycjom. Jeśli ciągi $\langle i_1, \ldots, i_r \rangle$, $\langle j_1, \ldots, j_r \rangle$ pokrywały się na q pozycjach ($q < r$), to ciągi $\langle i_1, \ldots, i_{h-1}, j_h, i_{h+1}, \ldots, i_r \rangle$, $\langle j_1, \ldots, j_r \rangle$ pokrywają się na $q+1$ pozycjach, jako że $j_h \neq i_h$. Powtarzając naszą konstrukcję albo znajdujemy żądany selektor częściowy $S_1 \cup \{y\}$, albo też sprowadzamy zagadnienie do sytuacji, w której $\langle i_1, \ldots, i_r \rangle = \langle j_1, \ldots, j_r \rangle$. Lecz w tym ostatnim przypadku istnieje pewne $h \in \{r+1, \ldots, p+1\}$ takie, że $j_h \notin \{i_1, \ldots, i_p\}$, nie może bowiem być $\{j_{r+1}, \ldots, j_{p+1}\} \subseteq \{i_{r+1}, \ldots, i_p\}$.

Wykonanie naszej konstrukcji jeszcze raz powoduje znalezienie żądanego selektora częściowego $S_1 \cup \{y\}$ ($y = y_h$). □

Dowód twierdzenia Edmondsa–Fulkersona dobrze ilustruje problemy, które występują przy znajdowaniu systemu reprezentantów. Załóżmy, że dla ciągu $\langle A_1, \ldots, A_n \rangle$ istnieje system reprezentantów, i że znaleźliśmy już system reprezentantów $\langle x_1, \ldots, x_k \rangle$ ($k < n$) dla $\langle A_1, \ldots, A_k \rangle$. Chociaż selektor częściowy $\{x_1, \ldots, x_k\}$ można wtedy rozszerzyć — na mocy twierdzenia Edmondsa–Fulkersona — do pewnego większego selektora częściowego, to jednak systemu $\langle x_1, \ldots, x_k \rangle$ nie można na ogół rozszerzyć do żadnego systemu reprezentantów $\langle x_1, \ldots, x_k, x \rangle$ dla $\langle A_1, \ldots, A_k, A_p \rangle$, $p > k$ (może bowiem zachodzić przypadek $A_{k+1}, \ldots, A_n \subseteq \{x_1, \ldots, x_k\}$). Przyjrzyjmy się jednak bliżej naszej konstrukcji. Zbiór $\{x_1, \ldots, x_k\}$ jest selektorem częściowym dla ciągu $\langle A_1, \ldots, A_k, A_{k+1} \rangle$. Skoro ten ostatni ciąg ma selektor, więc na mocy twierdzenia Edmondsa–Fulkersona ma on też selektor postaci $\{x_1, \ldots, x_k, x_{k+1}\}$. Otrzymujemy stąd następujący

WNIOSEK 8.3. *Załóżmy, że dla ciągu $\langle A_1, \ldots, A_n \rangle$ istnieje system reprezentantów, oraz niech $\langle x_1, \ldots, x_k \rangle$ będzie pewnym systemem reprezentantów dla $\langle A_1, \ldots, A_k \rangle$,*

$k < n$. Wtedy istnieje element x_{k+1} oraz permutacja σ zbioru $\{1, \ldots, k+1\}$ taka, że $\langle x_{\sigma(1)}, \ldots, x_{\sigma(k+1)} \rangle$ jest systemem reprezentantów dla $\langle A_1, \ldots, A_{k+1} \rangle$. □

Innym ważnym wnioskiem z twierdzenia Edmondsa–Fulkersona jest następujące

TWIERDZENIE 8.4. *Niech $\langle A_1, \ldots, A_n \rangle$ będzie ciągiem podzbiorów zbioru X. Wówczas wszystkie maksymalne selektory częściowe tego ciągu mają tę samą liczność. Ogólniej, dla dowolnego zbioru $Y \subseteq X$ wszystkie selektory częściowe maksymalne w zbiorze selektorów częściowych zawartych w Y mają tę samą liczność.*

Dowód. Gdyby dla dwóch maksymalnych selektorów częściowych S_1, S_2 było $|S_1| < |S_2|$, to na mocy twierdzenia Edmondsa–Fulkersona można by rozszerzyć S_1 do pewnego selektora częściowego $S_1 \cup \{x\}$, $x \in S_2 \setminus S_1$, co przeczy maksymalności S_1. Druga część twierdzenia wynika z faktu, iż zbiór selektorów częściowych ciągu $\langle A_1, \ldots, A_n \rangle$ zawartych w Y pokrywa się ze zbiorem wszystkich selektorów częściowych ciągu $\langle A_1 \cap Y, \ldots, A_n \cap Y \rangle$. □

§ 9. Wspólne selektory dwóch rodzin zbiorów

Zajmiemy się obecnie następującym problemem: kiedy dla dwóch rodzin zbiorów $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ istnieje zbiór S będący selektorem zarówno jednej jak i drugiej rodziny? Zbiór taki będziemy nazywali *selektorem wspólnym* rodzin $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$. Zaczniemy od szczególnego przypadku, w którym zbiory jednej z rodzin są parami rozłączne. Warunek istnienia wspólnego selektora jest wtedy wyjątkowo prosty, sytuacja taka zaś występuje często w zastosowaniach; we wszystkich przykładach zastosowań w następnym paragrafie obie rodziny są podziałami pewnego zbioru. Bez zmniejszenia ogólności możemy zakładać, że $A_1 \cup \ldots \cup A_n = B_1 \cup \ldots \cup B_n$, gdyż w przeciwnym przypadku możemy rozpatrywać rodziny $(A_1 \cap Y, \ldots, A_n \cap Y)$, $(B_1 \cap Y, \ldots, B_n \cap Y)$, gdzie $Y = (A_1 \cup \ldots \cup A_n) \cap (B_1 \cup \ldots \cup B_n)$.

TWIERDZENIE 9.1. *Niech*

$$X = A_1 \dot\cup \ldots \dot\cup A_n = B_1 \cup \ldots \cup B_n.$$

Następujące warunki są wtedy równoważne:

(a) *Rodziny $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ mają wspólny selektor.*

(b) *Suma dowolnych k zbiorów spośród $A_1, \ldots, A_n$ zawiera co najwyżej k zbiorów spośród $B_1, \ldots, B_n$ $(1 \leqslant k \leqslant n)$.*

(c) *Suma dowolnych k zbiorów spośród $B_1, \ldots, B_n$ ma niepuste przecięcie z co najmniej k zbiorami spośród $A_1, \ldots, A_n$ $(1 \leqslant k \leqslant n)$,*

(d) *Suma dowolnych k spośród zbiorów $B_1, \ldots, B_n$ ma niepuste przecięcie z co najwyżej k zbiorami spośród $A_1, \ldots, A_n$ $(1 \leqslant k \leqslant n)$.*

Dowód. (a)$\Rightarrow$(b). Załóżmy, że rodziny $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ mają wspólny selektor. Suma k zbiorów spośród $A_1, \ldots, A_n$ zawiera dokładnie k elementów tego selektora. Z drugiej strony, suma $l > k$ zbiorów spośród $B_1, \ldots, B_n$ zawiera w sumie co najmniej l elementów selektora. Tak więc suma k zbiorów spośród $A_1, \ldots, A_n$ może zawierać co najwyżej k zbiorów spośród $B_1, \ldots, B_n$.

(b)$\Rightarrow$(c). Udowodnimy, że z zaprzeczenia (c) wynika zaprzeczenie (b). Załóżmy zatem, że $B_{i_1} \cup \ldots \cup B_{i_k}$ ma niepuste przecięcie ze zbiorami $A_{j_1}, \ldots, A_{j_p}$, $p < k$ (i tylko z nimi). Wówczas $A_{j_1} \cup \ldots \cup A_{j_p} \supseteq B_{i_1} \cup \ldots \cup B_{i_k}$, co przeczy (b).

(c)$\Rightarrow$(a) Zauważmy, że (c) jest dokładnie warunkiem Halla dla rodziny $(C_1, \ldots, C_n)$ podzbiorów zbioru $\{1, \ldots, n\}$, gdzie

$$C_i = \{j\colon 1 \leqslant j \leqslant n \wedge B_i \cap A_j \neq \emptyset\}, \qquad 1 \leqslant i \leqslant n.$$

Na mocy twierdzenia Halla z (c) wynika istnienie selektora dla $(C_1, \ldots, C_n)$, tzn. takiej permutacji φ zbioru $\{1, \ldots, n\}$, że

$$B_1 \cap A_{\varphi(1)} \neq \emptyset, \quad \ldots, \quad B_n \cap A_{\varphi(n)} \neq \emptyset. \tag{9.1}$$

Wybierzmy z powyższych zbiorów po jednym elemencie:

$$x_1 \in B_1 \cap A_{\varphi(1)}, \ldots, x_n \in B_n \cap A_{\varphi(n)}.$$

Wobec rozłączności zbiorów $A_1, \ldots, A_n$ elementy $x_1, \ldots, x_n$ są parami różn Zbiór $\{x_1, \ldots, x_n\}$ jest więc wspólnym selektorem dla rodzin $(A_1, \ldots, A_n)$ $(B_1, \ldots, B_n)$.

(c)$\Leftrightarrow$(d). Istotnie, (d) jest niczym innym jak warunkiem Halla dla rodz $(C_1^*, \ldots, C_n^*)$, gdzie

$$C_i^* = \{j\colon 1 \leqslant j \leqslant n \wedge A_i \cap B_j \neq \emptyset\}, \qquad 1 \leqslant i \leqslant n.$$

Tak więc (d) jest równoważne istnieniu permutacji ψ takiej, że

$$A_1 \cap B_{\psi(1)} \neq \emptyset, \quad \ldots, \quad A_n \cap B_{\psi(n)} \neq \emptyset,$$

czyli

$$B_1 \cap A_{\psi^{-1}(1)} \neq \emptyset, \quad \ldots, \quad B_n \cap A_{\psi^{-1}(n)} \neq \emptyset. \tag{9.2}$$

Równoważność (c)$\Leftrightarrow$(d) jest teraz widoczna — wystarczy porównać (z (9.2). □

Specjalizując założenia twierdzenia 9.1 otrzymujemy następujący wnio ważny dla zastosowań:

TWIERDZENIE 9.2. *Niech $(A_1, \ldots, A_n)$, $(B_1, \ldots, B_n)$ będą dwoma podziałami zb X takimi, że $|A_i| = |B_i| = m$ dla $1 \leqslant i \leqslant n$ $(mn = |X|)$. Wówczas rod $(A_1, \ldots, A_n)$, $(B_1, \ldots, B_n)$ mają wspólny selektor. Co więcej, zbiór X mo przedstawić w postaci sumy rozłącznej m takich wspólnych selektorów.*

Dowód. Warunek (b) z twierdzenia 9.1 jest automatycznie spełniony: sum zbiorów spośród $A_1, \ldots, A_n$ liczy km elementów, nie może więc zawierać więcej

k zbiorów spośród $B_1, \ldots, B_n$. Na mocy twierdzenia 9.1 rodziny $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ mają więc wspólny selektor. Zauważmy, że jeśli S jest wspólnym selektorem rodzin $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$, to rodziny $(A_1 \setminus S, \ldots, A_n \setminus S)$ i $(B_1 \setminus S, \ldots, B_n \setminus S)$ spełniają założenia twierdzenia, a więc mają wspólny selektor. Drugą część twierdzenia otrzymujemy więc przez m-krotne zastosowanie pierwszej. □

Przejdźmy teraz do przypadku ogólnego, tzn. sytuacji, w której $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ są dowolnymi rodzinami (skończonych) zbiorów.

TWIERDZENIE 9.3 (Ford i Fulkerson [1]). *Rodziny* $(A_1, \ldots, A_n)$ *i* $(B_1, \ldots, B_n)$ *mają wspólny selektor wtedy i tylko wtedy, gdy*

$$\Big|\bigcup_{i\in I} A_i \cap \bigcup_{j\in J} B_j\Big| \geqslant |I|+|J|-n \tag{9.3}$$

dla dowolnych $I, J \subseteq \{1, \ldots, n\}$.

Dowód. Oryginalny dowód Forda i Fulkersona oparty był na teorii przepływów w sieciach. Podamy tu inny dowód, pochodzący od H. Perfect [1].

Konieczność warunku (9.3) jest prosta. Wystarczy zauważyć, że zbiór $\bigcup_{i\in I} A_i$ zawiera co najmniej $|I|$ elementów selektora, zaś zbiór $\bigcup_{j\in J} B_j$ co najmniej $|J|$ elementów selektora. Selektor liczy sobie n elementów, zatem liczność przecięcia $\bigcup_{i\in I} A_i \cap \bigcup_{j\in J} A_j$ wynosi co najmniej $|I|+|J|-n$.

W celu dowiedzenia dostateczności załóżmy, że $A_i, B_i \subseteq X = \{x_1, \ldots, x_m\}$ dla $1 \leqslant i \leqslant n$. Niech A i B będą odpowiednio macierzami incydencji rodzin $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$. Utwórzmy następującą macierz wymiaru $(m+n)\times$ $\times(m+n)$:

$$C = \left[\begin{array}{c|cccc} & 1 & & & \\ & & 1 & & \\ A & & & \ddots & \\ & & & & 1 \\ \hline 0 & & B^T & & \end{array}\right]$$

Wykażemy najpierw, że rodziny $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$ mają wspólny selektor wtedy i tylko wtedy, gdy w macierzy C istnieje rozproszony zbiór $m+n$ jedynek (tzn. zawierający dokładnie jedną jedynkę w każdej linii). Załóżmy, że taki rozproszony zbiór jedynek istnieje. Niech w pierwszych n kolumnach macierzy C jedynki z tego zbioru występują w wierszach o numerach $i_1, \ldots, i_n$. Z postaci macierzy C wynika wtedy, że w kolumnach o numerach $n+i_1, \ldots, n+i_n$ jedynki z naszego zbioru rozproszonego występują w wierszach o numerach $j_1, \ldots, j_n$, gdzie $\{j_1, \ldots, j_n\} = \{m+1, \ldots, m+n\}$. Łatwo zauważyć, że oznacza to, iż

zbiór $\{x_{i_1}, \ldots, x_{i_n}\}$ jest wspólnym selektorem dla $(A_1, \ldots, A_n)$ i $(B_1, \ldots, B_n)$. Równie łatwo jest znaleźć zbiór rozproszony $m+n$ jedynek mając pewien wspólny selektor $\{x_{i_1}, \ldots, x_{i_n}\}$. Zbiór ten zawiera n jedynek w podmacierzy A, n jedynek w podmacierzy B^T i $m-n$ jedynek w pozycjach $\langle j, n+j\rangle$, $j \in \{1, \ldots, m\} \setminus \{i_1, \ldots, i_n\}$ macierzy C (szczegóły pozostawiamy Czytelnikowi).

Wystarczy teraz wykazać, że z warunku (9.3) wynika istnienie zbioru rozproszonego jedynek liczności $m+n$ w macierzy C. W tym celu przypuśćmy, że wszystkie jedynki w C pokryliśmy liniami. Niech przez podmacierz A przechodzi r wierszy i s kolumn, przez podmacierz B^T zaś p wierszy i q kolumn tego pokrycia. Niech I będzie zbiorem numerów pozostałych $n-s$ kolumn przechodzących przez podmacierz A, J zaś zbiorem numerów pozostałych $n-p$ wierszy przechodzących przez podmacierz B^T (zakładamy tu, że wiersze tej podmacierzy numerowane są od 1 do n, a nie od $m+1$ do $m+n$). Oszacujemy teraz $r+s+p+q$, czyli liczbę linii naszego pokrycia. Zauważmy w tym celu, że r wierszy pokrycia przechodzących przez podmacierz A musi pokrywać wszystkie jedynki znajdujące się w kolumnach o numerach z I. Podobnie q kolumn pokrycia przechodzących przez B^T musi pokrywać wszystkie jedynki znajdujące się w wierszach tej podmacierzy o numerach z J. Wspomniane r wierszy i q kolumn pokrywa wszystkie m jedynek podmacierzy określonej przez pierwsze m wierszy i ostatnie m kolumn macierzy C. Tak więc $r+q-m$ spośród tych m jedynek pokrytych jest dwukrotnie — raz przez wiersz i raz przez kolumnę. Stąd i z (9.3) otrzymujemy

$$r+q-m \geqslant \Big|\bigcup_{i\in I} A_i \cap \bigcup_{j\in J} B_j\Big| \geqslant |I|+|J|-n = n-s+n-p-n = n-p-s,$$

czyli

$$r+s+p+q \geqslant m+n.$$

A zatem każde pokrycie jedynek macierzy C liniami ma liczność co najmniej $m+n$. Z twierdzenia węgierskiego (twierdzenie 1.6) wnioskujemy, że w C istnieje rozproszony zbiór jedynek o liczności $m+n$. Tym samym dowód jest zakończony. □

Warunki istnienia wspólnego selektora dla więcej niż dwóch rodzin zbiorów można znaleźć w pracach Browna [1, 2] i Longyeara [1].

§ 10. Zastosowania twierdzeń o wspólnych selektorach

Wszystkie zastosowania, które podamy w tym paragrafie, będą dotyczyły sytuacji, w której obie rodziny są podziałami pewnego zbioru na bloki o jednakowej liczności. Będziemy korzystali więc z twierdzenia 9.2.

Pierwsze zastosowanie dotyczy teorii grup. Przypomnijmy, że dla dowolnej podgrupy H grupy skończonej G rodzina $\{xH\colon x\in G\}$ — zwana rodziną *warstw lewostronnych* grupy G względem podgrupy H — jest podziałem grupy G na $|G|/|H|$ bloków o liczności $|H|$ (xH oznacza $\{xy\colon y\in H\}$). Podobnie rodzina $\{Hx\colon x\in G\}$ *warstw prawostronnych* jest podziałem na $|G|/|H|$ bloków o liczności

$|H|$. Podziały te są różne, jeśli H nie jest podgrupą normalną (por. np. Białynicki-Birula [1]). Na mocy twierdzenia 8.2 podziały te mają wspólny selektor. Fakt ten możemy sformułować nieco inaczej:

TWIERDZENIE 10.1. *Niech H będzie dowolną podgrupą grupy skończonej G i niech $m = |G|/|H|$. Wówczas istnieją elementy $z_1, \ldots, z_m \in G$ takie, że*

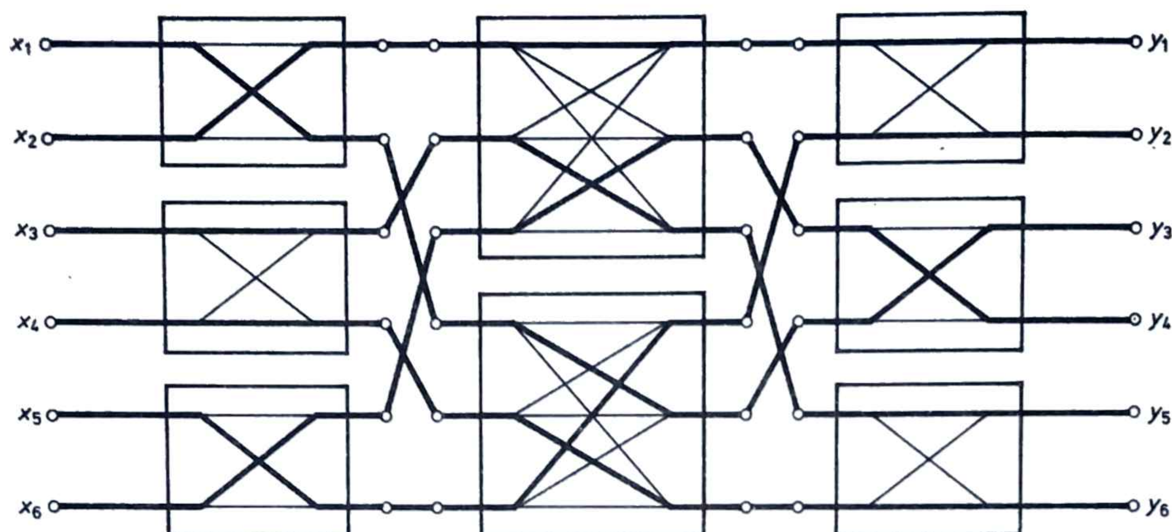
$$G = z_1 H \dot{\cup} \ldots \dot{\cup} z_m H = Hz_1 \dot{\cup} \ldots \dot{\cup} Hz_m.$$

Dowód. Twierdzenie wynika z poprzednich uwag, jeśli zauważymy, że dla dowolnych $z, x \in G$

$$z \in xH \Leftrightarrow zH = xH, \quad z \in Hx \Leftrightarrow Hz = Hx. \ \square$$

Wykażemy teraz zastosowanie twierdzenia o wspólnych selektorach do teorii sieci komutacyjnych stosowanych w telefonii. Wyobraźmy sobie, że mamy dwa zbiory „abonentów", każdy liczący N osób. Oznaczmy te zbiory przez X i Y. Chcemy zbudować urządzenie, które dla każdego wzajemnie jednoznacznego odwzorowania φ: $X \to Y$ połączy jednocześnie każdego abonenta $x \in X$ z abonentem $\varphi(x) \in Y$, i tylko z nim. Zakładamy, że podstawowymi elementami, z których mamy zbudować nasze urządzenie, są pojedyncze zestyki. Każdy zestyk ma dwie końcówki i może się znajdować w jednym z dwóch stanów — połączony lub rozłączony. Najprostszym rozwiązaniem, jakie się narzuca, jest połączenie zestykiem każdej pary abonentów $\langle x, y \rangle \in X \times Y$. Taką sieć o N^2 zestykach będziemy nazywali *komutatorem* wymiaru $N \times N$. Komutator taki ma N wejść (odpowiadających abonentom ze zbioru X) i N wyjść (odpowiadających abonentom ze zbioru Y). Aby „zrealizować" odwzorowanie φ: $X \to Y$, wystarczy, by zestyki łączące pary abonentów $\langle x, \varphi(x) \rangle$, $x \in X$, były połączone, pozostałe zaś zestyki rozłączone. Okazuje się, że nie jest to najlepsze — ze względu na liczbę zestyków — rozwiązanie. Inną strukturę sieci zaproponował C. Clos [1]. Aby ją opisać, załóżmy, że $N = n \cdot r$, gdzie $n > 1$, $r > 1$. *Sieć Closa* składa się z trzech sekcji. Pierwsza sekcja składa się z r komutatorów wymiaru $n \times n$, druga z n komutatorów wymiaru $r \times r$, trzecia zaś, tak jak pierwsza, z r komutatorów wymiaru $n \times n$. Sekcje połączone są ze sobą — pierwsza z drugą i druga z trzecią — w następujący sposób: i-te wyjście j-tego komutatora sekcji pierwszej jest połączone z j-tym wejściem i-tego komutatora sekcji drugiej (dla $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant r$), podobnie i-te wejśie j-tego komutatora sekcji trzeciej jest połączone z j-tym wyjściem i-tego komutatora sekcji drugiej. Istotną cechą tych połączeń jest to, że każdy komutator sekcji środkowej jest połączony ze wszystkimi komutatorami sekcji pierwszej i ze wszystkimi komutatorami sekcji trzeciej. Sieć Closa dla $n = 2$, $r = 3$ pokazano na rys. 22. Wykażemy teraz, że sieć Closa o N wejściach może służyć temu samemu celowi co komutator wymiaru $N \times N$.

TWIERDZENIE 10.2 (Slepian [1], Duguid [1]). *Za pomocą trójsekcyjnej sieci Closa o zbiorze wejść X i zbiorze wyjść Y można zrealizować połączenia odpowiadające dowolnemu wzajemnie jednoznacznemu odwzorowaniu φ: $X \to Y$.*



Rys. 22. Trójsekcyjna sieć Closa ($n = 3$, $r = 3$). Grubszą linią zaznaczona została realizacja odwzorowania $\varphi(x_1) = y_3$, $\varphi(x_2) = y_1$, $\varphi(x_3) = y_5$, $\varphi(x_4) = y_6$, $\varphi(x_5) = y_2$, $\varphi(x_6) = y_4$

Dowód. Niech A_i będzie zbiorem wejść i-tego komutatora sekcji pierwszej, C_i zbiorem wyjść i-tego komutatora sekcji trzeciej, zaś $B_i = \{x \in X\colon \varphi(x) \in C_i\}$ ($1 \leqslant i \leqslant r$). Wówczas $(A_1, \ldots, A_r)$ i $(B_1, \ldots, B_r)$ są dwoma podziałami zbioru X na bloki o liczności n. Na mocy twierdzenia 9.2 zbiór X można przedstawić w postaci $X = X_1 \dot{\cup} \ldots \dot{\cup} X_n$, gdzie zbiory $X_1, \ldots, X_n$ są wspólnymi selektorami rodzin $(A_1, \ldots, A_r)$ i $(B_1, \ldots, B_r)$. Żądane połączenia odpowiadające odwzorowaniu φ możemy teraz zrealizować łącząc wejścia ze zbioru X_j z odpowiednimi wyjściami przez j-ty komutator sekcji środkowej ($1 \leqslant j \leqslant n$). Zauważmy w tym celu, że X_j jest postaci $\{x_1, \ldots, x_r\}$, gdzie $x_i \in A_i$ oraz $\varphi(x_i) \in C_{\sigma(i)}$ dla pewnej permutacji σ zbioru $\{1, \ldots, r\}$. Aby zrealizować połączenie x_i z $\varphi(x_i)$, łączymy najpierw x_i z j-tym wyjściem i-tego komutatora sekcji pierwszej, następnie i-te wejście z $\sigma(i)$-tym wyjściem j-tego komutatora sekcji drugiej, wreszcie j-te wejście z wyjściem $\varphi(x_i)$ $\sigma(i)$-tego komutatora sekcji trzeciej. Postępując tak ze wszystkimi zbiorami X_j otrzymujemy N parami rozłącznych dróg realizujących połączenia wejść z wyjściami zadane przez odwzorowanie φ. □

Przyglądając się przykładowi sieci Closa na rys. 22 można mieć wątpliwości w czym sieć Closa, która w tym przypadku zawiera 42 zestyki, jest lepsza od pojedynczego komutatora o $6 \cdot 6 = 36$ zestykach. Aby się przekonać o wyższości sieci Closa, zauważmy, że ogólnie zawiera ona $r \cdot n^2 + n \cdot r^2 + r \cdot n^2 = r \cdot n(2n+r) = N(2n+r)$ zestyków. Dla przykładu, możemy zbudować sieć Closa o n^2 wejściach i $3n^3$ zestykach zamiast n^4 zestyków w przypadku pojedynczego komutatora. Zysk może być jeszcze większy, jeśli zauważymy, że każdy komutator sieci Closa możemy zamienić znów na sieć Closa i postępowanie to można kontynuować rekurencyjnie. Łatwo sprawdzić, że można w ten sposób skonstruować sieć o $N = 2^k$ wejściach i $2(2\log_2 N - 1)N$ zestykach.

Ostatnim zastosowaniem twierdzenia 9.2, o jakim wspomnimy w tym para-

grafie, będzie zagadnienie układania rozkładów zajęć. Przypuśćmy, że należy przeprowadzić m zajęć. Każde zajęcie ma ściśle określonego wykładowcę i salę, w której ma się odbyć. Innymi słowy, dane są dwa podziały $\{W_1, \ldots, W_n\}$ i $\{S_1, \ldots, S_n\}$ zbioru zajęć X (W_i jest zbiorem zajęć prowadzonych przez i-tego wykładowcę, S_i zaś zbiorem zajęć odbywających się w i-tej sali; zakładamy dla uproszczenia, że liczba wykładowców jest równa liczbie sal). Układając rozkład zajęć staramy się znaleźć rozkład zbioru zajęć na sumę parami rozłącznych wspólnych selektorów rodzin $\{W_1, \ldots, W_n\}$ i $\{S_1, \ldots, S_n\}$. Jeśli $X = X_1 \dot{\cup} \ldots \dot{\cup} X_k$ ($k \cdot n = |X|$) jest takim rozkładem, a każde zajęcie trwa, powiedzmy, godzinę, to możemy zrealizować wszystkie zajęcia w ciągu k godzin, prowadząc w i-tej godzinie zajęcia ze zbioru X_i. Przy takim zaplanowaniu zajęć żadna z sal nie będzie niewykorzystana, a żaden z wykładowców nie będzie miał „okienka” w ciągu tych k godzin. Oczywiście, aby wspomniany rozkład $X = X_1 \dot{\cup} \ldots \dot{\cup} X_k$ istniał, musi być

$$|W_i| = |S_i| = k, \qquad 1 \leqslant i \leqslant n.$$

Na odwrót, jeśli powyższy warunek jest spełniony, to na mocy twierdzenia 9.2 istnieje rozkład zbioru X na sumę k parami rozłącznych selektorów rodzin $\{W_1, \ldots, W_n\}$ i $\{S_1, \ldots, S_n\}$. Niestety, formułując zagadnienie rozkładu zajęć nie pomyśleliśmy zupełnie o osobach uczęszczających na te zajęcia. Przy opisanym przez nas zaplanowaniu zajęć może się bowiem zdarzyć, że pewne osoby mogą być zainteresowane różnymi zajęciami odbywającymi się jednocześnie (zauważmy jednak, że tak nie może się zdarzyć, jeśli każdy wykładowca ma „swoich” słuchaczy, którzy uczęszczają tylko na jego zajęcia). W praktyce dochodzą jeszcze inne ograniczenia, które sprawiają, że układanie rozkładów zajęć jest problemem znacznie bardziej złożonym niż to wynika z prostego modelu, który tu został przedstawiony.

§ 11. Algorytm znajdowania systemu reprezentantów

Podane dotychczas twierdzenia niewiele dają nam wskazówek jak wyznaczyć system reprezentantów dla danego ciągu zbiorów. Dlatego też opiszemy teraz algorytm, pochodzący od Hopcrofta i Karpa [1], który konstruuje system reprezentantów dla dowolnego ciągu zbiorów, jeśli tylko taki system istnieje.

Algorytm ten wygodnie nam będzie opisać w języku teorii grafów. Każdemu systemowi reprezentantów $\langle x_1, \ldots, x_n\rangle$ dla ciągu $\langle A_1, \ldots, A_n\rangle$ podzbiorów zbioru X odpowiada wzajemnie jednoznacznie skojarzenie $\{\{x_1, y_1\}, \ldots, \{x_n, y_n\}\}$ w grafie dwudzielnym o zbiorze wierzchołków $X \cup \{y_1, \ldots, y_n\}$ ($y_i \notin X$, $1 \leqslant i \leqslant n$) i zbiorze krawędzi $E = \{\{x, y_i\}: 1 \leqslant i \leqslant n \wedge x \in A_i\}$.

Główną częścią algorytmu będzie procedura, która mając dane skojarzenie M konstruuje skojarzenie N takie, że $|N| = |M|+1$ (niekoniecznie $M \subseteq N$), jeśli tylko takie skojarzenie istnieje.

Niech $M = \{\{a_1, b_1\}, \ldots, \{a_k, b_k\}\}$ będzie skojarzeniem w dowolnym grafie $G = \langle V, E\rangle$. O wierzchołku $v \in V$ powiemy, że jest *wolny* dla M, jeśli $v \notin \{a_1, \ldots, a_k, b_1, \ldots, b_k\}$. Zbiór krawędzi postaci

$$P = \{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{2k-1}, v_{2k}\},$$

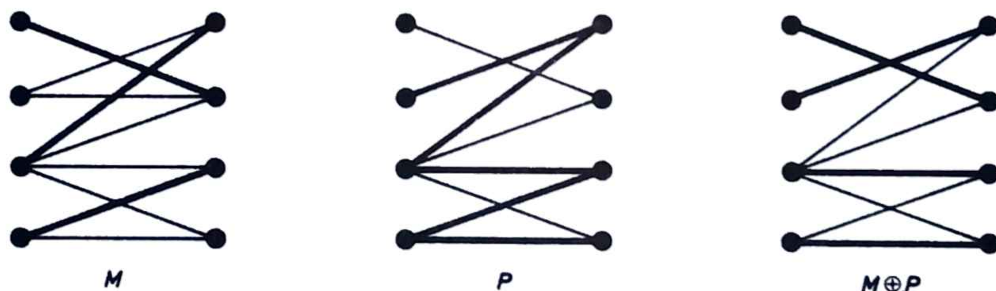
gdzie $k \geqslant 1$, wierzchołki $v_1, \ldots, v_{2k}$ są wszystkie różne, v_1 i v_{2k} są wolne dla M oraz

$$P \cap M = \{\{v_2, v_3\}, \{v_4, v_5\}, \ldots, \{v_{2k-2}, v_{2k-1}\}\},$$

będziemy nazywali *ścieżką naprzemienną względem* M (o zbiorze wierzchołków $\{v_1, \ldots, v_{2k}\}$ i długości $2k-1$).

LEMAT 11.1. *Niech M będzie skojarzeniem, P zaś ścieżką naprzemienną względem M. Wówczas $M \oplus P$ jest też skojarzeniem i $|M \oplus P| = |M|+1$ ($\oplus$ oznacza różnicę symetryczną: $M \oplus P = (M \setminus P) \cup (P \setminus M)$).*

Dowód. Łatwo zauważyć, że każdy wierzchołek $v \in V$ jest incydentny z co najwyżej jedną krawędzią z $M \oplus P$ (p. rys. 23).



Rys. 23. Przykład skojarzenia M, ścieżki naprzemiennej P względem M, wraz z odpowiadającym skojarzeniem $M \oplus P$

LEMAT 11.2. *Niech M i N będą skojarzeniami w grafie $G = \langle V, E\rangle$ i niech $|M| = r$, $|N| = s$, gdzie $s > r$. Wówczas $M \oplus N$ zawiera co najmniej $s-r$ ścieżek naprzemiennych względem M, o parami rozłącznych zbiorach wierzchołków.*

Dowód. Rozważmy graf $G' = \langle V, M \oplus N\rangle$. Każdy wierzchołek $v \in V$ jest incydentny z co najwyżej jedną krawędzią z $M \setminus N$ i z co najwyżej jedną krawędzią z $N \setminus M$ (gdyż M, N są skojarzeniami). Zatem każda składowa spójna grafu G' ma jedną z następujących trzech postaci:

(a) izolowany wierzchołek,

(b) cykl parzystej długości o krawędziach na przemian w $M \setminus N$ i $N \setminus M$,

(c) droga o krawędziach na przemian w $M \setminus N$ i $N \setminus M$.

Oznaczmy składowe spójne grafu G' przez $C_1, \ldots, C_p$, gdzie $C_i = \langle V_i, E_i\rangle$, i niech $\delta_i = |E_i \cap N| - |E_i \cap M|$. Mamy $\delta_i \in \{-1, 0, 1\}$, przy czym $\delta_i = 1$ wtedy i tylko wtedy, gdy C_i jest ścieżką naprzemienną względem M,

$$\sum_{i=1}^{p} \delta_i = \sum_{i=1}^{p} (|E_i \cap N| - |E_i \cap M|) = \sum_{i=1}^{p} |E_i \cap N| - \sum_{i=1}^{p} |E_i \cap M| =$$
$$= |N \setminus M| - |M \setminus N| = |N| - |M| = s - r.$$

Zatem $\delta_i = 1$ dla co najmniej $s-r$ wskaźników i, tzn. $M \oplus N$ zawiera co najmniej $s-r$ ścieżek naprzemiennych względem M, o parami rozłącznych zbiorach wierzchołków. □

WNIOSEK 11.3 (Berge). *Skojarzenie M grafu G ma maksymalną liczność wtedy i tylko wtedy, gdy nie istnieje w G ścieżka naprzemienna względem M.* □

Aby znaleźć skojarzenie o maksymalnej liczności (oznaczmy ją przez s) wystarczy zatem, startując od $M_0 = \emptyset$, znaleźć s razy ścieżkę naprzemienną P_i względem M_i i przyjąć $M_{i+1} = M_i \oplus P_i$. Aby bliżej przeanalizować ten proces potrzebnych nam będzie kilka lematów.

LEMAT 11.4. *Niech M będzie skojarzeniem, P najkrótszą ścieżką naprzemienną względem M, P' zaś ścieżką naprzemienną względem $M \oplus P$. Wówczas*

$$|P'| \geqslant |P| + 2|P \cap P'|.$$

Dowód. $N = M \oplus P \oplus P'$ jest skojarzeniem, przy czym $|N| = |M| + 2$. Na mocy lematu 11.2 zbiór $M \oplus N$ zawiera dwie ścieżki naprzemienne względem M, powiedzmy P_1 i P_2, o rozłącznych zbiorach wierzchołków. Mamy $M \oplus N = M \oplus M \oplus P \oplus P' = P \oplus P'$, zatem $|P \oplus P'| \geqslant |P_1| + |P_2|$. Lecz $|P_1| + |P_2| \geqslant 2|P|$, gdyż P jest najkrótszą ścieżką naprzemienną względem M. Stąd $|P \oplus P'| \geqslant 2|P|$. Z drugiej strony mamy oczywiście $|P \oplus P'| = |P| + |P'| - 2|P \cap P'|$. Równość ta w połączeniu z poprzednią nierównością daje $|P'| \geqslant |P| + 2|P \cap P'|$. □

LEMAT 11.5. *Niech s będzie maksymalną licznością skojarzenia w grafie G. Rozważmy ciągi $M_0, M_1, \ldots, M_s$ oraz $P_0, P_1, \ldots, P_{s-1}$, gdzie $M_0 = \emptyset$, P_i jest najkrótszą ścieżką naprzemienną względem M_i (takich najkrótszych ścieżek może być wiele) oraz $M_{i+1} = M_i \oplus P_i$ dla $0 \leqslant i \leqslant s-1$. Wówczas*

(a) *$|P_i| \leqslant |P_j|$ dla $i < j$.*

(b) *Jeśli $i < j$ oraz $|P_i| = |P_j|$, to ścieżki P_i, P_j mają rozłączne zbiory wierzchołków.*

(c) *Ciąg $|P_0|, |P_1|, \ldots, |P_{s-1}|$ zawiera co najwyżej $2\lfloor\sqrt{s}\rfloor + 2$ różnych liczb.*

Dowód. (a) wynika bezpośrednio z lematu 11.4.

(b) Załóżmy, że $|P_i| = |P_j|$, $i < j$, oraz że ścieżki P_i, P_j nie mają rozłącznych zbiorów wierzchołków. Bez zmniejszenia ogólności możemy przyjąć, że każda ścieżka P_m $(i < m < j)$ nie ma wspólnego wierzchołka ani z P_i ani z P_j. (Gdyby np. ścieżki P_i, P_m miały wspólny wierzchołek, to zamieniamy P_j na P_m; rozumowanie to wystarczy powtórzyć skończoną liczbę razy.) Łatwo zauważyć, że P_j jest ścieżką naprzemienną względem $M_i \oplus P_i$. Na mocy lematu 11.4 mamy $|P_j| \geqslant |P_i| + 2|P_i \cap P_j|$, a stąd, wobec $|P_i| = |P_j|$, wnioskujemy, iż ścieżki P_i, P_j nie mają

wspólnych krawędzi. Lecz z drugiej strony, jeśli v jest wspólnym wierzchołkiem dla P_i i P_j, to ta krawędź ze zbioru $M_i \oplus P_i$, która jest incydentna z v, jest wspólna dla P_i oraz P_j. Tak więc założenie o istnieniu wspólnego wierzchołka dla ścieżek P_i, P_j doprowadziło nas do sprzeczności.

(c) Niech $r = \lfloor s - \sqrt{s} \rfloor$. Mamy $|M_r| = r$, a zatem na mocy lematu 11.2 istnieje co najmniej $s-r$ rozłącznych ścieżek naprzemiennych względem M_r. Istnieje więc ścieżka, która ma nie więcej niż $r/(s-r)$ krawędzi w M_r. Długość takiej ścieżki nie przekracza $2r/(s-r)+1$. Skoro P_r jest najkrótszą ścieżką naprzemienną względem M_r, otrzymujemy

$$|P_r| \leqslant 2\lfloor s - \sqrt{s} \rfloor / (s - \lfloor s - \sqrt{s} \rfloor) + 1 =$$
$$= 2(s - \lceil \sqrt{s} \rceil)/\lceil \sqrt{s} \rceil + 1 = 2s/\lceil \sqrt{s} \rceil - 1 \leqslant$$
$$\leqslant 2\sqrt{s} - 1 \leqslant 2\lfloor \sqrt{s} \rfloor + 1.$$

Każda ścieżka naprzemienna ma długość nieparzystą, tak więc dla każdego $i \leqslant r$ długość ścieżki P_i jest jedną z $\lfloor \sqrt{s} \rfloor + 1$ liczb nieparzystych nie przekraczających $2\lfloor \sqrt{s} \rfloor + 1$. Wśród liczb $|P_{r+1}|, \ldots, |P_s|$ może być co najwyżej $s - r = \lceil \sqrt{s} \rceil$ różnych, a zatem liczba różnych długości reprezentowanych przez ścieżki $P_0, \ldots, P_s$ nie przekracza $\lfloor \sqrt{s} \rfloor + 1 + \lceil \sqrt{s} \rceil \leqslant 2\lfloor \sqrt{s} \rfloor + 2$. □

Istotą algorytmu Hopcrofta–Karpa – najszybszego ze znanych algorytmów znajdowania skojarzenia o maksymalnej liczności w grafie dwudzielnym – jest to, że w jednym kroku znajdowane są wszystkie ścieżki P_i o tej samej długości. Ogólny schemat tego algorytmu jest następujący:

Algorytm Hopcrofta–Karpa

Dane: Graf niezorientowany $G = \langle V, E \rangle$.

Wynik: Skojarzenie M o maksymalnej liczności.

Krok 1. $M := \emptyset$.*

Krok 2. Niech $l(M)$ będzie długością najkrótszej ścieżki naprzemiennej względem M ($l(M) = \infty$, jeśli nie istnieje żadna taka ścieżka). Jeśli $l(M) = \infty$, to M jest żądanym skojarzeniem o maksymalnej liczności i działanie algorytmu jest zakończone. Jeśli $l(M) \neq \infty$, to znajdź maksymalny zbiór $\{Q_1, \ldots, Q_t\}$ ścieżek naprzemiennych względem M o następujących własnościach: (a) Każda ścieżka Q_i ma długość $l(M)$. (b) Ścieżki $Q_1, \ldots, Q_t$ mają parami rozłączne zbiory wierzchołków.

Krok 3. $M := M \oplus Q_1 \oplus \ldots \oplus Q_t$, przejdź do kroku 2.

TWIERDZENIE 11.6. *Jeśli maksymalna liczność skojarzenia w grafie G wynosi s, to algorytm Hopcrofta–Karpa konstruuje taki zbiór wykonując krok 2 nie więcej niż $2\lfloor \sqrt{s} \rfloor + 2$ razy.*

---

* Wykonanie instrukcji $M := e$, gdzie e jest pewnym wyrażeniem, powoduje obliczenie wartości tego wyrażenia i przyjęcie zmiennej M jako tymczasowej nazwy tej wartości, aż do momentu wykonania innej instrukcji $M := e'$.

Dowód. Zbiór $\{Q_1, \ldots, Q_t\}$ ścieżek długości $l(M)$ konstruowany w kroku 2 jest maksymalny, a zatem, na mocy lematu 11.5(b) każda ścieżka naprzemienna dla $M \oplus Q_1 \oplus \ldots \oplus Q_t$ ma długość większą niż $l(M)$. Tak więc wartość $l(M)$ rośnie w każdym kolejnym wykonaniu kroku 2. Z lematu 10.5(c) wynika, że może być co najwyżej $2\lfloor\sqrt{s}\rfloor+2$ różnych wartości $l(M)$, zatem krok ten może być wykonywany najwyżej $2\lfloor\sqrt{s}\rfloor+2$ razy. Lecz jedyną sytuacją, w jakiej algorytm się zatrzymuje, jest $l(M) = \infty$ w kroku 2. Na mocy wniosku 11.3 M jest wtedy skojarzeniem o maksymalnej liczności. □

Zauważmy, że wszystkie dotychczasowe rozważania stosowały się do dowolnego grafu niezorientowanego, niekoniecznie dwudzielnego. Pokażemy teraz sposób efektywnej realizacji kroku 2 korzystający w istotny sposób z dwudzielności grafu.

Załóżmy zatem, że zbiór wierzchołków naszego grafu $G = \langle V, E\rangle$ jest sumą rozłączną zbiorów X i Y, przy czym każda krawędź jest postaci $\{x, y\}$, $x \in X$, $y \in Y$. Niech $M \subseteq E$ będzie skojarzeniem w grafie G. Jeśli każdą krawędź $\{x, y\} \in M$ ($x \in X$, $y \in Y$) zastąpimy krawędzią $\langle x, y\rangle$ zorientowaną od X do Y, każdą zaś krawędź z $E \setminus M$ zorientujemy od Y do X, to otrzymamy graf zorientowany $\vec{G} = \langle V, \vec{E}\rangle$ o tej własności, że ścieżki naprzemienne względem M w G odpowiadają jednoznacznie drogom zorientowanym w $\vec{G}$ łączącym wierzchołki $y \in Y$ wolne dla M z wierzchołkami $x \in X$ wolnymi dla M. Ponieważ będą nas interesowały zawsze tylko najkrótsze ścieżki naprzemienne, wyodrębnimy z $\vec{G}$ pewien podgraf G^*, w którym wspomniane drogi zorientowane odpowiadają jednoznacznie najkrótszym ścieżkom naprzemiennym względem M.

Aby skonstruować G^*, postępujemy w następujący sposób: Niech L_0 będzie zbiorem tych elementów z Y, które są wolne dla M. Określamy teraz ciągi V_0, V_1, $V_2, \ldots$ i E_0, E_1, $E_2, \ldots$ następująco:

$$V_{i+1} = \{v \in V \setminus (V_0 \cup \ldots \cup V_i)\colon \text{ istnieje } u \in V_i \text{ takie, że } \langle u, v\rangle \in \vec{E}\},$$

$$E_{i+1} = \{\langle u, v\rangle \in \vec{E}\colon u \in V_i \wedge v \in V_{i+1}\}.$$

Konstrukcję tę prowadzimy aż do momentu, gdy V_i zawiera pewien wierzchołek $v \in X$ wolny dla M. Niech i^* będzie najmniejszym wskaźnikiem i, dla którego to następuje. Nasz graf $G^* = \langle V^*, E^*\rangle$ definiujemy następująco:

$$V^* = V_0 \cup \ldots \cup V_{i^*-1} \cup \{v \in V_{i^*}\colon v \text{ wolny dla } M\},$$

$$E^* = E_0 \cup \ldots \cup E_{i^*-2} \cup \{\langle u, v\rangle \in E_{i^*-1}\colon v \text{ wolny dla } M\}.$$

Łatwo zauważyć, że V_i jest zbiorem tych wierzchołków, których odległość w $\vec{G}$ od V_0 jest równa i (przez *odległość* wierzchołka v od zbioru wierzchołków V_0 rozumiemy długość najkrótszej drogi łączącej v z pewnym wierzchołkiem z V_0). Mamy poza tym $V_i \subseteq Y$ dla i parzystych oraz $V_i \subseteq X$ dla i nieparzystych. Najkrótsze ścieżki naprzemienne względem M odpowiadają jednoznacznie drogom (o długości $i^* = l(M)$) od V_0 do V_{i^*} w G^*. Aby znaleźć maksymalny zbiór takich

dróg o parami rozłącznych zbiorach wierzchołków, wygodnie nam będzie dołączyć do G^* dwa nowe wierzchołki s, t oraz krawędzie $\langle s, v\rangle$ dla wszystkich $v \in V_0$, i $\langle u, t\rangle$ dla wszystkich $u \in V_{i^\circ}$ wolnych dla M. Oznaczmy otrzymany graf przez $G' = \langle V', E'\rangle$. A oto zapowiedziany algorytm:

Algorytm konstruowania maksymalnego zbioru dróg

Dane: Graf $G' = \langle V', E'\rangle$ opisany powyżej. Graf ten dany jest w postaci list (ciągów) $L(v)$, $v \in V'$, gdzie każda lista $L(v)$ zawiera wierzchołki ze zbioru $\{u \in V' \colon \langle v, u\rangle \in E'\}$ uporządkowane w dowolny sposób.

Wynik: Maksymalny zbiór dróg od s do t, z których żadne dwie nie mają wspólnych wierzchołków różnych od s, t.

Krok 1. $B := \emptyset$. (B składa się w każdej chwili z wierzchołków dróg wygenerowanych do tej chwili, bez wierzchołków s, t, oraz z wierzchołków, o których wiadomo, że do żadnej takiej drogi należeć nie mogą.)

Krok 2. Połóż s na stosie*. (Na stosie znajduje się zawsze pewien ciąg wierzchołków, który w dalszym ciągu może zostać przedłużony do jednej z szukanych dróg od s do t).

Krok 3. Jeśli stos jest pusty, to działanie algorytmu jest zakończone. W przeciwnym przypadku $g :=$ górny element stosu.

Krok 4. Jeśli lista $L(g)$ jest pusta, to zdejmij g ze stosu i przejdź do kroku 3. $p :=$ pierwszy element listy $L(g)$. Usuń p z listy $L(g)$.

Krok 5. Jeśli $p \in B$, to przejdź do kroku 4. Połóż p na stosie. Jeśli $p \neq t$, to $B := B \cup \{p\}$, $g := p$ i przejdź do kroku 4. Odczytaj elementy ze stosu (od dołu do góry) jako ciąg wierzchołków następnej znalezionej drogi od s do t. Usuń ze stosu wszystkie elementy i przejdź do kroku 2.

Istotę tego algorytmu można opisać tak: Startujemy z $s_0 = s$, rozważamy pewną krawędź $\langle s_0, s_1\rangle$ (s_1 jest pierwszym elementem listy $L(s_0)$), następnie pewną krawędź $\langle s_1, s_2\rangle$ itd. Ciąg $s_0, s_1, s_2, \ldots$ zapamiętujemy na stosie. Za każdym razem rozważając krawędź $\langle s_i, s_{i+1}\rangle$ usuwamy ją z grafu (tzn. usuwamy s_{i+1} z $L(s_i)$), gdyż krawędź ta albo należy do pewnej drogi, której początek dany jest przez ciąg $s_0, s_1, \ldots, s_i, s_{i+1}$, i która zostanie przez algorytm znaleziona, albo też nie należy do żadnej drogi prowadzącej od s do t (i rozłącznej z poprzednio znalezionymi drogami). Podobnie każdy nowy napotkany wierzchołek jest od razu eliminowany z dalszych rozważań (tzn. dodawany do zbioru B). Jeśli na pewnym kroku lista $L(s_i)$ jest pusta (tzn. jeśli naszej drogi nie da się przedłużyć), cofamy się o jeden wierzchołek wstecz (zdejmujemy s_i ze stosu) i próbujemy następnej krawędzi odchodzącej od s_{i-1}. Działanie algorytmu jest zakończone, gdy s jest usuwane ze stosu, po stwierdzeniu, iż lista $L(s)$ jest pusta. Żadna nowa droga od s do t wtedy oczywiście nie istnieje. Łatwo zauważyć, że własność natychmiastowej

---

* Stos można sobie wyobrażać jako pewien ciąg. Położenie elementu na stosie oznacza dopisanie go na końcu ciągu, zdjęcie zaś górnego elementu stosu oznacza usunięcie ostatniego elementu ciągu. Zakładamy, że na początku działania algorytmu stos jest pusty.

eliminacji każdego „nowego" wierzchołka i każdej „nowej" krawędzi powoduje, iż liczba elementarnych operacji jest ograniczona przez $C_1(|V'|+|E'|)$, gdzie C_1 jest pewną stałą (niezależną od G').

Zauważmy, że skonstruowanie grafu G' na podstawie grafu G może być dokonane przez $C_2(|V|+|E|)$ operacji (aby znaleźć V_{i+1}, wystarczy przejrzeć wszystkie listy $L(v)$, $v \in V_i$, przy czym żadna z tych list nie będzie drugi raz rozważana). Tak więc całkowita liczba operacji w algorytmie Hopcrofta–Karpa może być oszacowana przez

$$(2\sqrt{|V|}+1)(C_1+C_2)(|V|+|E|) \leqslant C_3\sqrt{|V|}(|V|+|E|),$$

lub też przez $C_4|V|^{5/2}$ dla odpowiednich stałych C_3 i C_4.

Powracając do naszego zagadnienia znajdowania systemu reprezentantów dla ciągu $\langle A_1, \ldots, A_n \rangle$ podzbiorów zbioru X ($|X| = m$), i biorąc pod uwagę, jak ciągowi temu przyporządkowujemy graf, widzimy, że liczba elementarnych kroków potrzebnych do znalezienia systemu reprezentantów przez algorytm Hopcrofta–Karpa może być oszacowana przez $C_5\sqrt{n}(n+m+\sum_{i=1}^{n}|A_i|)$ dla pewnej stałej C_5. Jeśli zbiory A_i są niepuste i $\bigcup_{i=1}^{n} A_i = X$ (do sytuacji takiej można łatwo doprowadzić), to $m, n \leqslant \sum_{i=1}^{n}|A_i|$ i otrzymujemy ostatecznie oszacowanie $C\sqrt{n}\sum_{i=1}^{n}|A_i|$ dla pewnej stałej C.

Oczywiście rozważania powyższe nie pretendują do pełnej ścisłości, jako że nie zdefiniowaliśmy precyzyjnie pojęć związanych z algorytmami, takich jak np. „krok elementarny". Czytelnika pragnącego te rozważania uściślić odsyłamy do bogatej literatury dotyczącej złożoności obliczeniowej algorytmów kombinatorycznych (p. np. Aho, Hopcroft i Ullman [1], Banachowski i Kreczmar [1], Lipski [1]).

§ 12. Zasada selekcji Rado i wersje nieskończone niektórych twierdzeń

Udowodnimy teraz pewną nieskończoną wersję twierdzenia Halla. Najpierw jednak musimy sprecyzować, co rozumiemy przez system reprezentantów nieskończonej rodziny zbiorów. Niech I będzie dowolnym zbiorem i niech $\langle A_i \rangle_{i\in I}$ będzie dowolną indeksowaną rodziną zbiorów, tzn. funkcją F określoną na zbiorze I taką, że $F(i) = A_i$ dla każdego $i \in I$. Dowolną funkcję $f \in \times_{i\in I} A_i$ będziemy nazywali *funkcją wyboru* dla $\langle A_i \rangle_{i\in I}$. Funkcję taką oznaczamy czasem przez $\langle a_i \rangle_{i\in I}$, gdzie $a_i = f(i)$. Przez *system reprezentantów* dla $\langle A_i \rangle_{i\in I}$ będziemy rozumieli dowolną różnowartościową funkcję wyboru. Do dowodu zapowiedzianej nieskoń-

czonej wersji twierdzenia Halla potrzebne nam będzie pewne ogólne twierdzenie pochodzące od Rado [3]. Przypomnijmy, że przez $J \subseteq_{\text{fin}} I$ oznaczamy fakt, że J jest skończonym podzbiorem zbioru I.

TWIERDZENIE 12.1 (zasada selekcji Rado). *Niech $\langle A_i \rangle_{i \in I}$ będzie dowolną rodziną indeksowaną zbiorów skończonych i dla każdego $J \subseteq_{\text{fin}} I$ niech f_J będzie funkcją wyboru dla $\langle A_i \rangle_{i \in J}$ („lokalną funkcją wyboru"). Wówczas istnieje funkcja wyboru f dla $\langle A_i \rangle_{i \in I}$ („globalna funkcja wyboru") taka, że dla dowolnego $J \subseteq_{\text{fin}} I$ istnieje $K \subseteq_{\text{fin}} I$ takie, że $J \subseteq K$ i $f \upharpoonright J = f_K \upharpoonright J$.*

Dowód (Gottschalk [1]). Skorzystamy z twierdzenia Tichonowa (p. np. Kuratowski i Mostowski [1]). Jeśli każdy ze zbiorów A_i wyposażymy w topologię dyskretną (tzn. taką, w której każdy podzbiór jest otwarty), to, wobec skończoności, zbiór A_i staje się zwartą przestrzenią topologiczną. Produkt $X = \bigtimes_{i \in I} A_i$ jest, na mocy twierdzenia Tichonowa, przestrzenią zwartą w topologii produktowej (por. Kuratowski i Mostowski [1]).

Dla każdego $J \subseteq_{\text{fin}} I$ niech

$$F_J = \{f \in X\colon \text{ istnieje } K \text{ takie, że } J \subseteq K \subseteq_{\text{fin}} I \text{ i } f \upharpoonright J = f_K \upharpoonright J\}.$$

Oczywiście $F_J \neq \emptyset$. Wykażemy, że zbiory F_J są domknięte. Istotnie,

$$X \setminus F_J = \{f \in X\colon \text{ dla każdego } K\, (J \subseteq K \subseteq_{\text{fin}} I \Rightarrow f \upharpoonright J \neq f_K \upharpoonright J)\}$$

i łatwo zauważyć, że dla każdego elementu $f \in X \setminus F_J$ zbiór $X \setminus F_J$ zawiera też podzbiór

$$G_J(f) = \{g \in X\colon g \upharpoonright J = f \upharpoonright J\} = \bigtimes_{i \in I} A_i^*,$$

gdzie

$$A_i^* = \begin{cases} \{f(i)\}, & \text{jeśli } i \in J, \\ A_i & \text{jeśli } i \notin J. \end{cases}$$

Na mocy definicji topologii produktowej oraz skończoności zbioru J podzbiór $G_J(f)$ jest otwarty. Zbiór $X \setminus F_J = \bigcup_{f \in X \setminus F_J} G_J(f)$ jest więc otwarty i w konsekwencji F_J jest zbiorem domkniętym. Przecięcie dowolnej skończonej liczby zbiorów postaci F_J jest niepuste, gdyż

$$F_{J_1} \cap \ldots \cap F_{J_k} \supseteq F_{J_1 \cup \ldots \cup J_k} \neq \emptyset.$$

Na mocy zwartości przestrzeni X przecięcie wszystkich zbiorów postaci F_J jest też niepuste. Lecz każda funkcja $f \in \bigcap_{J \subseteq_{\text{fin}} I} F_J$ jest globalną funkcją wyboru, której istnienie orzeka twierdzenie. □

UWAGA 12.2. ***Jeśli wszystkie lokalne funkcje wyboru są różnowartościowe, to każda globalna funkcja wyboru jest też różnowartościowa.***

Dowód. Jeśli dla pewnej globalnej funkcji wyboru f byłoby $f(i)=f(j)$, $i \neq j$, to istniałby zbiór K taki, że $J=\{i, j\} \subseteq K \subseteq_{\text{fin}} I$ oraz $f_K(i)=f_K(j)$, a więc sprzeczność. □

A oto zapowiedziana nieskończona wersja twierdzenia Halla:

Twierdzenie 12.3 (M. Hall [2]). *Niech $\langle A_i \rangle_{i\in I}$ będzie dowolną rodziną indeksowaną zbiorów skończonych. Rodzina ta ma system reprezentantów wtedy i tylko wtedy, gdy każda jej skończona podrodzina $\langle A_i \rangle_{i\in J}$, $J \subseteq_{\text{fin}} I$ spełnia warunek Halla.*

Dowód. Na mocy twierdzenia Halla (twierdzenie 3.1), każda skończona podrodzina $\langle A_i \rangle_{i\in J}$ ma system reprezentantów, tzn. dla każdego $J \subseteq_{\text{fin}} I$ istnieje różnowartościowa lokalna funkcja wyboru f_J. Twierdzenie wynika więc bezpośrednio z zasady selekcji Rado i uwagi 12.2. □

Niestety, łatwo podać przykład wskazujący, że twierdzenie to przestaje być prawdziwe, nawet gdy tylko jeden ze zbiorów A_i jest nieskończony.

Nie jest znany żaden prosty warunek konieczny i dostateczny na to, by dowolna rodzina zbiorów miała system reprezentantów, mimo dość intensywnych badań w tej dziedzinie (p. np. Damerell i Milner [1]).

Klasycznym zastosowaniem twierdzenia 12.3 jest dowód równoliczności baz przestrzeni liniowej. Przypomnijmy, że bazą przestrzeni liniowej L nazywamy dowolny podzbiór $B \subseteq L$ taki, że każdy element $x\in L$ wyraża się jednoznacznie jako (skończona) kombinacja liniowa elementów z B.

Twierdzenie 12.4. *Niech L będzie przestrzenią liniową nad ciałem F, oraz niech B i C będą dwiema bazami tej przestrzeni. Wówczas $|B| = |C|$.*

Dowód. Każdy element $b\in B$ ma jednoznaczne rozwinięcie postaci $\sum_{i=1}^{n} a_i c_i$, gdzie $c_i \in C$, $a_i \in F$, $a_i \neq 0$. Niech C_b oznacza zbiór tych elementów bazy C, które występują w rozwinięciu elementu b względem bazy C (tzn. $C_b = \{c_1, \ldots, c_n\}$). Oczywiście każdy zbiór C_b jest skończony. Wykażemy, że każda skończona podrodzina rodziny $\langle C_b \rangle_{b\in B}$ spełnia warunek Halla. Istotnie, $|C_{b_1} \cup \ldots \cup C_{b_k}| < k$ oznaczałoby, iż każdy spośród liniowo niezależnych wektorów $b_1, \ldots, b_k$ wyraża się jako kombinacja liniowa elementów co najwyżej $(k-1)$-elementowego zbioru $C_{b_1} \cup \ldots \cup C_{b_k}$, co jest oczywiście niemożliwe. Na mocy twierdzenia 12.3 istnieje więc funkcja różnowartościowa $f\colon B \to C$. Wobec symetrii istnieje również różnowartościowa funkcja $g\colon C \to B$. Wobec twierdzenia Cantora–Bernsteina (p. rozdz. 1, zad. 9) $|C| = |B|$. □

Zasada selekcji ma wiele ciekawych zastosowań, nie tylko w zagadnieniach dotyczących systemów reprezentantów (por. np. Mirsky [1]). Używamy jej zwykle w sytuacjach, gdy trzeba wykazać, iż pewna własność ma „skończony charakter".

Na zakończenie tego paragrafu podamy następujące wzmocnienie twierdzenia Dilwortha, prawdziwe dla dowolnego – niekoniecznie skończonego – zbioru częściowo uporządkowanego.

TWIERDZENIE 12.5. *Niech $\langle P, \leqslant \rangle$ będzie dowolnym zbiorem częściowo uporządkowanym. Jeśli maksymalna liczność antyłańcucha w $\langle P, \leqslant \rangle$ jest skończona, to jest ona równa minimalnej liczbie łańcuchów, które pokrywają P.*

Dowód. Niech maksymalna liczność antyłańcucha w $\langle P, \leqslant \rangle$ będzie skończona, równa m. Wystarczy wykazać, że istnieje podział zbioru P na m łańcuchów. Na mocy „skończonego" twierdzenia Dilwortha, dla każdego $Q \subseteq_{\text{fin}} P$ istnieje podział zbioru Q na m łańcuchów, $Q = L_1 \dot{\cup} \ldots \dot{\cup} L_m$ (nie zakładamy, że wszystkie te łańcuchy są niepuste). Podziałowi temu możemy przyporządkować funkcję $f_Q\colon Q \to \{1, \ldots, m\}$ określoną przez $f_Q(x) = i \Leftrightarrow x \in L_i$ $(1 \leqslant i \leqslant m, x \in Q)$. Stosując zasadę selekcji Rado dla funkcji lokalnych f_Q, $Q \subseteq_{\text{fin}} P$ otrzymujemy pewną globalną funkcję wyboru $f\colon P \to \{1, \ldots, m\}$. Mamy $P = P_1 \dot{\cup} \ldots \dot{\cup} P_m$, gdzie $P_i = \{x \in P\colon f(x) = i\}$ dla $1 \leqslant i \leqslant m$. Wystarczy teraz wykazać, że zbiory P_i są łańcuchami. Lecz jeśli $x, y \in P_i$ (tzn. $f(x) = f(y) = i$), to istnieje zbiór $Q \subseteq_{\text{fin}} P$ taki, że $\{x, y\} \subseteq Q$ i $f_Q \upharpoonright \{x, y\} = f \upharpoonright \{x, y\}$. W konsekwencji $f_Q(x) = f_Q(y) = i$, czyli $x, y \in L_i$, gdzie L_i jest łańcuchem podziału $Q = L_1 \dot{\cup} \ldots \dot{\cup} L_m$ odpowiadającego funkcji f_Q. Tak więc każde dwa elementy zbioru P_i są porównywalne, co oznacza iż P_i jest łańcuchem. □

Zadania

1. Udowodnić twierdzenie 1.5 nie korzystając z lematu 1.3.

Wskazówka: Każdemu wyrazowi a_i przyporządkować parę $\langle l(a_i), p(a_i)\rangle$, gdzie $l(a_i)$ jest maksymalną długością podciągu niemalejącego kończącego się na a_i, $p(a_i)$ zaś jest maksymalną długością podciągu malejącego rozpoczynającego się od a_i.

2. Podać przykład grafu (oczywiście niedwudzielnego), dla którego nie zachodzi odpowiednik twierdzenia 1.7.

3 (R. Rado [1]). Rodzina $\langle A_i \rangle_{i \in I}$ jest *dwudzielna*, jeśli istnieje podział $I = I_1 \dot{\cup} I_2$ taki, że $\langle A_i \rangle_{i \in I_1}$, jak również $\langle A_i \rangle_{i \in I_2}$ składa się z parami rozłącznych zbiorów. R jest *zbiorem reprezentującym* dla $\langle A_i \rangle_{i \in I}$, jeśli $A_i \cap R \neq \emptyset$ dla każdego $i \in I$. Udowodnić, że dla każdej skończonej dwudzielnej rodziny skończonych niepustych zbiorów minimalna liczność zbioru reprezentującego jest równa maksymalnej liczbie parami rozłącznych zbiorów tej rodziny.

Wskazówka: Skorzystać z twierdzenia Dilwortha.

4. Niech A będzie macierzą zero-jedynkową bez linii zerowych. Będziemy mówili, że dwie linie się *nie przecinają*, jeśli albo są równoległe, albo na ich skrzyżowaniu występuje 0. Udowodnić, że maksymalna liczba nie przecinających się linii jest równa minimalnej liczności zbioru jedynek, z których każda linia zawiera co najmniej jedną.

Wskazówka: Skorzystać z poprzedniego zadania.

5. W dowodzie twierdzenia 1.4 określiliśmy zbiór częściowo uporządkowany P o tej własności, że jeśli odwrócimy relację porządku $\leqslant$ między elementami ciągu $a_1, \ldots, a_n$, to otrzymamy pewien zbiór częściowo uporządkowany $\hat{P}$ taki, że łańcuchy w P są dokładnie antyłańcuchami w $\hat{P}$, zaś antyłańcuchy w P łańcuchami w $\hat{P}$. Udowodnić, że dla dowolnego skończonego zbioru częściowo uporządkowanego Q zbiór $\hat{Q}$ o powyższej własności istnieje wtedy i tylko wtedy, gdy Q jest izomorficzny ze zbiorem P odpowiadającym pewnemu ciągowi $a_1, \ldots, a_n$, gdzie $n = |P|$ (rozpatrujemy tu wyłącznie ciągi bez powtórzeń).

6. Udowodnić, że twierdzenie Spernera jest prawdziwe również dla zbiorów z powtórzeniami, w tym sensie, że najliczniejszą rodziną Spernera podzbiorów n-elementowego zbioru z powtórzeniami jest rodzina jego wszystkich podzbiorów $\lfloor n/2 \rfloor$-elementowych.

7. Rodzinę zbiorów nazywamy *r-rodziną Spernera*, jeśli nie zawiera ona łańcucha $(r+1)$-elementowego. Udowodnić, że jeśli $\{A_1, \ldots, A_m\}$ jest r-rodziną Spernera podzbiorów zbioru n-elementowego, to $\sum_{i=1}^{m} 1/\binom{n}{|A_i|} \leqslant r$.

8. (Erdős [1]). Wykazać, że liczność dowolnej r-rodziny Spernera (por. poprzednie zadanie) podzbiorów zbioru n-elementowego jest nie większa od sumy r największych współczynników dwumiennych, tzn. od $\sum_{i=1}^{r} \binom{n}{\lfloor (n+i)/2 \rfloor}$.

9. Udowodnić następujące wzmocnienie twierdzenia Spernera: Niech $\{X_1, X_2\}$ będzie podziałem zbioru X i niech $\{A_1, \ldots, A_m\}$ będzie rodziną taką, że dla żadnych $i \neq j$, $1 \leqslant i, j \leqslant m$, nie jest spełniony warunek:

$$A_i \cap X_1 = A_j \cap X_1 \wedge A_i \cap X_2 \subseteq A_j \cap X_2$$

lub

$$A_i \cap X_1 \subseteq A_j \cap X_1 \wedge A_i \cap X_2 = A_j \cap X_2.$$

Wówczas $m \leqslant \binom{n}{\lfloor n/2 \rfloor}$.

10. Udowodnić, że w dowolnym podziale rodziny $\mathscr{P}(X)$ na łańcuchy symetryczne liczba łańcuchów liczności k jest równa $\binom{n}{\lfloor (n+k)/2 \rfloor} - \binom{n}{\lceil (n+k+1)/2 \rceil}$ $(n = |X|,\ 1 \leqslant k \leqslant n)$.

11. (Dilworth [2]). Niech $\langle P, \leqslant \rangle$ będzie skończonym zbiorem częściowo uporządkowanym, $\mathfrak{A}(P)$ zaś rodziną jego wszystkich antyłańcuchów. Uporządkujmy $\mathfrak{A}(P)$ przyjmując $A \leqslant B$, jeśli dla każdego $a \in A$ istnieje $b \in B$ takie, że $a \leqslant b$. Udowodnić, że $\langle \mathfrak{A}(P), \leqslant \rangle$ jest kratą rozdzielną, zaś rodzina wszystkich antyłańcuchów maksymalnej liczności jest jej podkratą.

12. Udowodnić, że liczność $\mathfrak{A}(P)$ (p. poprzednie zadanie) jest równa liczbie monotonicznych funkcji boolowskich f: $\{0, 1\}^n \to \{0, 1\}$, $n = |P|$.

13. Udowodnić, że każda rodzina Spernera $\mathscr{F} \subseteq \mathscr{P}(X)$ o maksymalnej liczności jest postaci $\mathscr{P}_{\lfloor n/2 \rfloor}(X)$ lub $\mathscr{P}_{\lceil n/2 \rceil}(X)$ $(n = |X|)$.

14. Udowodnić, że istnieje zbiór $\binom{n}{\lfloor n/2 \rfloor}$ permutacji zbioru $X = \{1, \ldots, n\}$ taki, że każdy $Y \subseteq X$ występuje jako „odcinek początkowy" w pewnej z tych permutacji (permutację φ: $\{1, \ldots, n\} \to \{1, \ldots, n\}$ identyfikujemy z ciągiem $\langle \varphi(1), \ldots, \varphi(n) \rangle$).

15. *Nieujemną ścieżką kratową długości n* od $\langle 0, 0 \rangle$ do $\langle n, p \rangle$ nazywamy ciąg $\langle 0, 0 \rangle = \langle 0, m_0 \rangle$, $\langle 1, m_1 \rangle, \ldots, \langle n, m_n \rangle = \langle n, p \rangle$, gdzie $m_i \geqslant 0$, $|m_i - m_{i-1}| = 1$ dla $1 \leqslant i \leqslant n$. (a) Udowodnić, że istnieje dokładnie $\binom{n}{\lfloor n/2 \rfloor}$ nieujemnych ścieżek kratowych długości n. (b) („Twierdzenie Bertranda o tajnym głosowaniu") Wykazać, że jeśli $k = (n-p)/2$ jest liczbą całkowitą, to liczba nieujemnych ścieżek kratowych od $\langle 0, 0 \rangle$ do $\langle n, p \rangle$ jest równa $\binom{n}{k} - \binom{n}{k-1} = \lfloor (n-2k+1)/(n-k+1) \rfloor \binom{n}{k}$.

16. Niech $1 \leqslant k \leqslant r \leqslant 2k$. Udowodnić, że jeśli $\mathscr{F}$ jest rodziną Spernera złożoną z podzbiorów właściwych o licznościach co najmniej k zbioru r-elementowego X taką, że suma żadnych dwóch zbiorów z $\mathscr{F}$ nie daje X, to $|\mathscr{F}| \leqslant \binom{r-1}{k}$.

17. Dla danego $J_0 \subseteq \{1, \ldots, n\}$, $J_0 \neq \emptyset$, podać przykład ciągu $\langle A_1, \ldots, A_n \rangle$, który nie ma systemu reprezentantów, lecz który spełnia warunek $|\bigcup_{i \in J} A_i| \geqslant |J|$ dla wszystkich $J \subseteq \{1, \ldots, n\}$, $J \neq J_0$.

18. Wykazać, że warunek Halla dla ciągu $\langle A_1, \ldots, A_n \rangle$ podzbiorów zbioru X jest równoważny następującemu warunkowi: $|\{i\colon A_i \subseteq Y\}| \leqslant |Y|$ dla każdego $Y \subseteq X$.

19. Wyprowadzić twierdzenie Halla z twierdzenia węgierskiego. (Rozpatrzyć graf dwudzielny o zbiorze wierzchołków $\{1, \ldots, n\} \cup X$, $X = \bigcup_{i=1}^{n} A_i$, gdzie $\{i, x\}$ jest krawędzią wtedy i tylko wtedy, gdy $x \in A_i$.)

20. (J. S. Pym). Nie korzystając z twierdzenia Dilwortha wyprowadzić z twierdzenia Halla następujący wniosek: Jeśli A, B są dwoma antyłańcuchami o maksymalnej liczności, to $A \cup B$ jest sumą n łańcuchów, gdzie $n = |A| = |B|$.

21. Wykazać, że ciąg $\langle A_1, \ldots, A_n \rangle$ podzbiorów zbioru X ma system reprezentantów wtedy i tylko wtedy, gdy

$$\sum_{i \in I} |A_i \cap Y| \geqslant |I| + |Y| - |X|$$

dla każdego $I \subseteq \{1, \ldots, n\}$, $Y \subseteq X$.

22. Niech A będzie macierzą zero-jedynkową. Wykazać, że per $A = 1$ wtedy i tylko wtedy, gdy istnieje macierz permutacyjna P taka, że PAP^T ma na głównej przekątnej same jedynki, zaś ponad główną przekątną same zera.

23. Wykazać, że dla macierzy kwadratowych zachodzi równość per $A =$ per A^T.

24. Czy per $AB =$ per A per B dla dowolnych macierzy kwadratowych A, B?

25. Wykazać, że dla dowolnej macierzy kwadratowej A o współczynnikach rzeczywistych nieujemnych per $A \geqslant |\det A|$.

26. Sformułować odpowiednik rozwinięcia Laplace'a dla per A, gdzie A jest dowolną (niekoniecznie kwadratową) macierzą.

27. Korzystając z wniosku 5.5 wykazać, że

(a) $n! = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^n$,

(b) $D_n = \sum_{r=0}^{n-1} (-1)^r \binom{n}{r} (n-r)^r (n-r-1)^{n-r}$,

gdzie D_n jest liczbą nieporządków (tzn. takich permutacji σ zbioru $\{1, \ldots, n\}$, że $\sigma(i) \neq i$ dla $1 \leqslant i \leqslant n$.por. rozdz. 1, twierdzenie 7.4).

28. Udowodnić twierdzenie 4.4 dla macierzy o elementach z dowolnego ciała.

29. Wykazać, że jeśli B powstaje z A przez pomnożenie pewnego wiersza (kolumny) przez c, to per $B = c$ per A.

30. Wykazać, że dodanie do pewnego wiersza (kolumny) kombinacji liniowej pozostałych wierszy (kolumn) zmienia na ogół wartość permanentu.

31. Wykazać, że dla dowolnego $k \geqslant 2$ istnieje macierz A wymiaru $n \times n$ taka, że per $A = k$ i $n \leqslant \lfloor \log_2 (k-1) \rfloor + 2$.

32. Udowodnić, że jeśli A jest macierzą bistochastyczną, to $0 <$ per $A \leqslant 1$, przy czym per $A = 1$ wtedy i tylko wtedy, gdy A jest macierzą permutacyjną.

33. Przeprowadzić szczegółowy dowód twierdzenia 5.2 przyjmując, że elementy macierzy A są dowolnymi nieujemnymi liczbami całkowitymi (niekoniecznie 0 lub 1).

34. Podać teoriografową interpretację twierdzenia 5.2 przyjmując, że A odpowiada pewnemu grafowi dwudzielnemu o zbiorze wierzchołków $\{x_1, \ldots, x_n\} \cup \{y_1, \ldots, y_n\}$ (x_i jest połączone z y_j wtedy i tylko wtedy, gdy $a_{ij} = 1$).

35. Niech „·" będzie działaniem binarnym określonym na elementach zbioru $X = \{x_1, \ldots, x_n\}$. Systemowi $\langle X, \cdot \rangle$ możemy przyporządkować *tablicę Cayley'a*, tzn. macierz $A = [a_{ij}]$ wymiaru $n \times n$, gdzie $a_{ij} = x_i \cdot x_j$. System $\langle X, \cdot \rangle$ nazywamy *kwazigrupą*, jeśli dla dowolnych $a, b \in X$ każde z równań $ax = b$, $ay = b$ ma dokładnie jedno rozwiązanie. Wykazać, że macierz kwadratowa jest kwadratem łacińskim wtedy i tylko wtedy, gdy jest tablicą Cayley'a pewnej kwazigrupy (przy oczywistym rozszerzeniu pojęcia kwadratu łacińskiego rzędu n na macierze o elementach z dowolnego zbioru n-elementowego).

36. Wykazać, że kwadrat łaciński $L = [a_{ij}]$ jest tablicą Cayley'a (por. poprzednie zadanie) grupy (tzn. kwazigrupy łącznej) wtedy i tylko wtedy, gdy dla dowolnych $i, j, k, l, i_1, j_1, k_1, l_1$

$$(a_{ik} = a_{i_1k_1} \wedge a_{il} = a_{i_1l_1} \wedge a_{jk} = a_{j_1k_1}) \Rightarrow a_{jl} = a_{j_1l_1}.$$

37. Wykazać, że jeśli $n \geqslant 2t$, to dowolny prostokąt łaciński typu $\langle t, t, n \rangle$ rozszerza się do kwadratu łacińskiego rzędu n.

38. Niech $(A_1, \ldots, A_n)$ ma selektor. Wykazać, że selektor ten jest jedyny wtedy i tylko wtedy, gdy $|A_1 \cup \ldots \cup A_n| = n$.

39. Wykazać, że zbiór $Y \subseteq X$ jest selektorem częściowym rodziny $(A_1, \ldots, A_n)$ podzbiorów zbioru X wtedy i tylko wtedy, gdy każdy zbiór $Z \subseteq Y$ przecina co najmniej $|Z|$ zbiorów spośród $A_1, \ldots, A_n$, tzn. $|\{i\colon A_i \cap Z \neq \emptyset\}| \geqslant |Z|$.

Wskazówka: Zastosować twierdzenie Halla do rodziny dualnej, tzn. takiej, której macierz incydencji jest transponowana względem macierzy incydencji rodziny $(A_1, \ldots, A_n)$.

40. Udowodnić, że rodzina $(A_1, \ldots, A_n)$ podzbiorów zbioru X ma selektor częściowy o liczności r wtedy i tylko wtedy, gdy

$$|\{i\colon A_i \cap Y \neq \emptyset\}| \geqslant |Y| + r - |X|$$

dla każdego $Y \subseteq X$. Zastanowić się nad dualnymi wersjami innych twierdzeń (np. twierdzenia Edmondsa–Fulkersona).

41. Udowodnić następujące twierdzenie. Niech Y będzie selektorem częściowym rodziny $(A_1, \ldots, A_n)$ podzbiorów zbioru X, oraz niech podrodzina $(B_1, \ldots, B_k) \subseteq (A_1, \ldots, A_n)$ ma selektor. Udowodnić, że istnieje wtedy zbiór Z oraz rodzina $(C_1, \ldots, C_r)$ taka, że $Y \subseteq Z \subseteq X$, $(B_1, \ldots, B_k) \subseteq (C_1, \ldots, C_r) \subseteq (A_1, \ldots, A_n)$ oraz Z jest selektorem rodziny $(C_1, \ldots, C_r)$. W konsekwencji, jeśli Y jest maksymalnym selektorem, $(B_1, \ldots, B_k)$ zaś maksymalną podrodziną mającą selektor, to Y jest jej selektorem.

42. Udowodnić, że dla każdej rodziny $(A_1, \ldots, A_n)$ istnieje podrodzina $(B_1, \ldots, B_k)$ taka, że zbiór maksymalnych selektorów częściowych rodziny $(A_1, \ldots, A_n)$ pokrywa się ze zbiorem selektorów rodziny $(B_1, \ldots, B_k)$, przy czym jako $(B_1, \ldots, B_k)$ można przyjąć dowolną maksymalną podrodzinę rodziny $(A_1, \ldots, A_n)$ mającą selektor.

43. Wykazać, że selektor częściowy $S \subseteq X$ rodziny $(A_1, \ldots, A_n)$ jest maksymalny wtedy i tylko wtedy, gdy dla każdego $y \in X \setminus S$ dla każdej podrodziny $(B_1, \ldots, B_k)$, której S jest selektorem, i każdego zbioru A_i zawierającego element y mamy $A_i \in (B_1, \ldots, B_k)$.

44. Wykazać, że Y jest selektorem częściowym rodziny $(A_1, \ldots, A_n)$ wtedy i tylko wtedy, gdy

$$\Big|Y \cap \bigcup_{j \in J} A_j\Big| \geqslant |J| + |Y| - n$$

dla dowolnego $J \subseteq \{1, \ldots, n\}$.

45. Wyprowadzić twierdzenie Halla–Ore z twierdzenia Königa.

46 (J. Q. Longyear [1]). Niech A będzie zbiorem skończonym, s, t zaś ustalonymi liczbami naturalnymi. Niech $P_1, \ldots, P_t$ będą podziałami zbioru A na s bloków „rozdzielającymi punkty", tzn. takimi, że dla dowolnych $x, y \in A$, $x \neq y$, istnieje podział $P_j = (B_1, \ldots, B_s)$ oraz jego dwa bloki B_p, B_q

$(p \neq q)$ takie, że $x \in B_p$, $y \in B_q$. Udowodnić, że jeśli $|A| > s^t - s^{t-1}$, to istnieje wspólny selektor dla $P_1, \ldots, P_t$.

47 (T. C. Brown [1]). Udowodnić, że twierdzenie z poprzedniego zadania pozostaje prawdziwe, jeśli każda z rodzin P_j ma postać $(B_1, \ldots, B_s)$, $\bigcup_{i=1}^{s} B_i = A$ (lecz niekoniecznie $B_p \cap B_q = \emptyset$ dla $p \neq q$). Wykazać, że ograniczenie $s^t - s^{t-1}$ nie może być poprawione.

48. Wyprowadzić wniosek 7.3 z wniosku 10.3.

49. Podać algorytm znajdowania wspólnego selektora dla dwu podziałów i oszacować wykonywaną przez niego liczbę operacji elementarnych (jako funkcję wymiaru problemu).

ROZDZIAŁ 5

WŁASNOŚCI PODZIAŁOWE

Intuicja mówi nam, że jeśli „duży" zbiór podzielimy na „niewielką" liczbę części, to jedna z tych części będzie „spora". Odwrotnie, jeśli chcemy, by przy dowolnym podziale zbioru na pewną liczbę części któraś z nich była „spora", wystarczy żądać, by zbiór był dostatecznie „duży". Najprostszym faktem wyrażającym tę intuicję jest

Zasada szufladkowa Dirichleta. Jeśli $X = X_1 \cup \ldots \cup X_t$ i $|X| \geqslant t+1$, to $|X_i| \geqslant 2$ dla pewnego $i \in \{1, \ldots t\}$.

Dowód tej zasady, przez indukcję, jest banalny. Równie oczywiste jest następujące jej uogólnienie:

Zasada podziałowa. Niech $q_1, \ldots, q_t$ będzie ciągiem liczb naturalnych. Jeśli $X = X_1 \cup \ldots \cup X_t$ oraz $|X| \geqslant (\sum_{i=1}^{t} q_1) - t + 1$, to $|X_i| \geqslant q_i$ dla pewnego $i \in \{1, \ldots, t\}$.

Oczywiście zasada szufladkowa jest szczególnym przypadkiem zasady podziałowej ($q_i = 2$ dla $1 \leqslant i \leqslant t$).

W rozdziale tym będziemy się zajmowali różnymi uogólnieniami zasady podziałowej. W uogólnieniach tych zbiór X podlegający podziałowi wyposażony jest zwykle w pewną strukturę, w terminach której możemy uściślić nieformalne stwierdzenie „jedna z części, na jakie podzieliliśmy X, jest «spora»". W zagadnieniach, które będziemy rozważali, zbiór X będzie między innymi zbiorem podzbiorów r-elementowych pewnego innego zbioru (twierdzenie Ramsey'a), zbiorem krawędzi grafu (twierdzenie Deubera) oraz zbiorem liczb naturalnych (twierdzenie van der Waerdena i Schura).

§ 1. Twierdzenie Ramsey'a

Przypomnijmy, że dla dowolnego zbioru X przez $\mathscr{P}_r(X)$ oznaczamy rodzinę wszystkich jego r-elementowych podzbiorów. Daleko idącym uogólnieniem zasady podziałowej jest następujące

TWIERDZENIE 1.1 (Ramsey [1]). *Dla dowolnych* $r, t \in N$ *oraz dla dowolnego ciągu liczb naturalnych* $q_1, \ldots, q_t$ *istnieje liczba* n *o następującej własności:*

Ilekroć $|X| \geq n$ *oraz* $\mathscr{P}_r(X) = A_1 \cup \ldots \cup A_t$, *wówczas istnieje* $i \in \{1, \ldots, t\}$ *oraz zbiór* $Y \subseteq X$ *taki, że* $|Y| \geq q_i$ *i* $\mathscr{P}_r(Y) \subseteq A_i$.

Najmniejszą liczbę n o powyższej własności będziemy oznaczali przez $R_r(q_1, \ldots, q_t)$. Nim przejdziemy do dowodu tego twierdzenia – a podamy dwa różne dowody – przedyskutujemy własności liczb $R_r(q_1, \ldots, q_t)$ (zwane są one *liczbami Ramsey'a*).

Stosunkowo najprostsza jest interpretacja naszego twierdzenia, gdy $r = 2$. Zauważmy, że wystarczy dowieść twierdzenia dla przypadku, gdy rodzina $\{A_1, \ldots, A_t\}$ jest podziałem* zbioru $\mathscr{P}_r(X)$. W przypadku $r = 2$ podział zbioru $\mathscr{P}_r(X)$ to nic innego jak pokolorowanie krawędzi grafu pełnego, którego zbiorem wierzchołków jest X, t kolorami (mianowicie, jeśli $\{x, y\} \in A_i$, to mówimy, że krawędź łącząca x i y jest i-tego koloru). Przy takiej interpretacji twierdzenie Ramsey'a (dla $r = 2$) mówi nam, że jeśli liczba wierzchołków jest „dostatecznie duża" to istnieje „spory" podgraf pełny o krawędziach pokolorowanych jednym kolorem. Zauważmy jeszcze, że twierdzenie trywializuje się, jeśli $q_i < r$ dla pewnego i, lub jeśli $t = 1$.

Pierwszy dowód twierdzenia Ramsey'a. Zastosujemy indukcję względem r oraz t. Zauważmy najpierw, że z zasady podziałowej wynika, iż

$$R_1(q_1, \ldots, q_t) = \left(\sum_{i=1}^{t} q_i\right) - t + 1.$$

Wykażemy teraz, przez indukcję względem t, że prawdziwość naszego twierdzenia dla $t = 2$ (i dowolnych q_1, q_2) implikuje jego prawdziwość dla dowolnego $t > 2$. Istotnie, załóżmy że udowodniliśmy już twierdzenie dla $t = s$, oraz rozważmy dowolny ciąg $q_1, \ldots, q_s, q_{s+1}$. Wykażemy, że liczba Ramsey'a $R_r(q_1, \ldots, q_s, q_{s+1})$ istnieje – dokładniej, że

$$R_r(q_1, \ldots, q_s, q_{s+1}) \leq R_r(R_r(q_1, \ldots, q_s), q_{s+1}).$$

Istotnie, zapisując dowolny rozkład

$$\mathscr{P}_r(X) = A_1 \cup \ldots \cup A_s \cup A_{s+1} \quad \text{jako} \quad \mathscr{P}_r(X) = (A_1 \cup \ldots \cup A_s) \cup A_{s+1}$$

widzimy, że dla $|X| \geq R_r(R_r(q_1, \ldots, q_s), q_{s+1})$ albo istnieje zbiór $Y_1 \subseteq X$ taki, że $|Y_1| \geq R_r(q_1, \ldots, q_s)$ i $\mathscr{P}_r(Y_1) \subseteq A_1 \cup \ldots \cup A_s$, albo istnieje zbiór $Y_2 \subseteq X$ taki, że $|Y_2| \geq q_{s+1}$ i $\mathscr{P}_r(Y_2) \subseteq A_{s+1}$ (nie wykluczamy oczywiście zachodzenia obu przypadków jednocześnie). Zajmijmy się bliżej tym pierwszym przypadkiem. Oznaczając $A_i' = A_i \cap \mathscr{P}_r(Y_1)$ mamy $\mathscr{P}_r(Y_1) = A_1' \cup \ldots \cup A_s'$, i wobec definicji

* W rozdziale tym mówiąc „podział $\{A_1, \ldots, A_t\}$" nie zakładamy, że wszystkie zbiory A_i są niepuste.

liczby Ramsey'a $R_r(q_1, \ldots, q_s)$ istnieje $i \in \{1, \ldots, s\}$ oraz zbiór $Z \subseteq Y_1$ taki, że $|Z| \geqslant q_i$ oraz $\mathscr{P}_r(Z) \subseteq A_i'$, tym bardziej więc $\mathscr{P}_r(Z) \subseteq A_i$. Na mocy zasady indukcji twierdzenie nasze jest prawdziwe dla dowolnych t, przy założeniu jego prawdziwości dla $t = 2$.

Dla $t = 2$ stosujemy indukcję względem q_1, q_2 oraz r. Założenie indukcyjne ma postać:

Istnieją liczby $n_1 = R_r(q_1 - 1, q_2)$, $n_2 = R_r(q_1, q_2 - 1)$ oraz dla dowolnych p_1, p_2 liczby $R_{r-1}(p_1, p_2)$. Z założenia tego wywnioskujemy istnienie liczby $R_r(q_1, q_2)$. Rozpoznajemy tu zasadę indukcji dla zbioru częściowo uporządkowanego trójek $\langle r, q_1, q_2 \rangle$, gdzie

$$\langle r', q_1', q_2' \rangle \leqslant \langle r, q_1, q_2 \rangle \Leftrightarrow r' < r \vee (r' = r \wedge q_1' \leqslant q_1 \wedge q_2' \leqslant q_2)$$

(p. rozdział 1, twierdzenie 2.3).

Zauważmy teraz, że wystarczy zająć się przypadkiem q_1, $q_2 > r$, bowiem $R_r(r, q_2) = q_2$. Istotnie, jeśli $|X| \geqslant q_2$, $\mathscr{P}_r(X) = A_1 \cup A_2$, to albo istnieje $Z \in A_1$ i wtedy $\mathscr{P}_r(Z) = \{Z\} \subseteq A_1$, albo $A_1 = \emptyset$, $A_2 = \mathscr{P}_r(X)$ i wtedy $\mathscr{P}_r(X) \subseteq A_2$. Analogicznie dowodzimy, że $R_r(q_1, r) = q_1$.

Wróćmy do naszego założenia indukcyjnego. Wynika z niego, w szczególności, istnienie liczby $n = R_{r-1}(n_1, n_2)$. Niech $|X| \geqslant n+1$ i niech $\mathscr{P}_r(X) = A_1 \cup A_2$. Obierzmy dowolny element $a \in X$ i oznaczmy $Z = X \setminus \{a\}$. Rozkład $\mathscr{P}_r(X) = A_1 \cup A_2$ indukuje rozkład $\mathscr{P}_{r-1}(Z) = B_1 \cup B_2$ następująco:

$$W \in B_i \Leftrightarrow W \cup \{a\} \in A_i \quad (i = 1, 2).$$

Skoro $|X| \geqslant n+1$, zatem $|Z| \geqslant n$, a więc na mocy założenia indukcyjnego zachodzi (co najmniej) jeden z następujących dwóch przypadków:

(1) Istnieje zbiór $V_1 \subseteq Z$ taki, że $|V_1| \geqslant n_1$ i $\mathscr{P}_{r-1}(V_1) \subseteq B_1$.

(2) Istnieje zbiór $V_2 \subseteq Z$ taki, że $|V_2| \geqslant n_2$ i $\mathscr{P}_{r-1}(V_2) \subseteq B_2$.

Rozpatrzymy tylko przypadek (1); w przypadku (2) postępujemy analogicznie.

Każdy rozkład $\mathscr{P}_r(X) = A_1 \cup A_2$ generuje rozkład $\mathscr{P}_r(V_1) = C_1 \cup C_2$, gdzie $C_i = A_i \cap \mathscr{P}_r(V_1)$ $(i = 1, 2)$. Skoro $|V_1| \geqslant n_1 = R_r(q_1 - 1, q_2)$, to albo (a) istnieje zbiór $T_1 \subseteq V_1$ taki, że $|T_1| \geqslant q_1 - 1$ i $\mathscr{P}_r(T_1) \subseteq C_1$, albo (b) istnieje zbiór $T_2 \subseteq V_1$ taki, że $|T_2| \geqslant q_2$ i $\mathscr{P}_r(T_2) \subseteq C_2$. Jeśli zachodzi (b), to za Y przyjmujemy T_2 i, skoro $C_2 \subseteq A_2$, otrzymujemy tezę. Niech przeto zachodzi (a). Wykażemy, że $\mathscr{P}_r(T_1 \cup \{a\}) \subseteq A_1$. Istotnie, jeśli $U \in \mathscr{P}_r(T_1 \cup \{a\})$, to albo $U \in \mathscr{P}_r(T_1)$, i wtedy $U \in C_1 \subseteq A_1$, albo $U \notin \mathscr{P}_r(T_1)$, czyli $U = W \cup \{a\}$, gdzie $W \in \mathscr{P}_{r-1}(T_1)$, czyli $U \in A_1$, na mocy definicji zbioru B_1. To kończy dowód dla przypadku (1). W przypadku (2) rozpatrujemy V_2 zamiast V_1, dalej postępując analogicznie. □

Podamy teraz zapowiadany drugi dowód twierdzenia Ramsey'a a (dla $r = 2$). W tym celu będziemy potrzebowali pewnych pojęć pomocniczych. Przez *drzewo* będziemy rozumieć dowolny zbiór częściowo uporządkowany $T = \langle X, \leqslant \rangle$, w którym istnieje element najmniejszy (zwany *korzeniem* drzewa) i dla każdego $x \in X$ zbiór $\{y \in X\colon y < x\}$ jest skończonym łańcuchem w T. Zgodnie z ogólną definicją rangi elementu w zbiorze częściowo uporządkowanym (por. roz. 1, § 2), ranga

dowolnego elementu x drzewa jest równa $r(x) = |\{y \in X\colon y < x\}|$. Korzeń jest jedynym elementem o randze 0. Zauważmy, że w drzewie każdy element oprócz korzenia ma dokładnie jednego bezpośredniego poprzednika. Jeśli y jest bezpośrednim poprzednikiem elementu x (przypomnijmy, że piszemy wtedy $y \lessdot x$), to $r(y) = r(x) - 1$.

W drzewie skończonym (tzn. o skończonym zbiorze X) każdy element ma skończoną liczbę bezpośrednich następników. *Rząd elementu* x, oznaczany przez $b(x)$, definiujemy jako liczbę bezpośrednich następników elementu x:

$$b(x) = |\{y \in X\colon x \lessdot y\}|.$$

Wysokość i *rząd drzewa* (skończonego) $T = \langle X, \leqslant\rangle$ określamy odpowiednio jako

$$r(T) = \max\{r(x)\colon x \in X\}, \qquad b(T) = \max\{b(x)\colon x \in X\}.$$

LEMAT 1.2. *Jeśli* $T = \langle X, \leqslant\rangle$ *jest drzewem takim, że* $b(T) \leqslant t$ *oraz* $|X| \geqslant (t^k - 1)/(t-1) + 1$, *to* $r(T) \geqslant k$.

D o w ó d. Dowodzimy, przez indukcję względem i, że w T jest co najwyżej t^i elementów o randze i. Dowód jest oczywisty, jako że mamy dokładnie $t^0 = 1$ element o randze 0 (korzeń), a elementów o randze $i+1$ jest co najwyżej t razy więcej niż elementów o randze i (każdy element o randze i ma co najwyżej t bezpośrednich następników).

Jeśliby nasze drzewo miało wysokość $r(T) \leqslant k-1$, to mielibyśmy $|X| \leqslant \sum_{i=0}^{k-1} t^i = (t^k - 1)/(t-1)$, wbrew założeniu. □

Drugi dowód twierdzenia Ramsey'a (dla $r = 2$). Załóżmy, że dane są liczby $t, q_1, \ldots, q_t$. Niech $|X| \geqslant (t^q - 1)/(t-1) + 1$, gdzie $q = \left(\sum_{i=1}^{t} (q_i - 1)\right) - t + 1 = \left(\sum_{i=1}^{t} q_i\right) - 2t + 1$, oraz niech $\mathscr{P}_2(X) = A_1 \dot\cup \ldots \dot\cup A_t$. Mamy wykazać, że istnieje $i \in \{1, \ldots, t\}$ oraz zbiór $Y \subseteq X$ taki, że $|Y| \geqslant q_i$ i $\mathscr{P}_2(Y) \subseteq A_i$.

Będziemy konstruowali drzewo $T = \langle D, \leqslant\rangle$, którego elementami będą pewne ciągi skończone postaci $i_1 \ldots i_p$, gdzie $p \geqslant 0$ oraz $1 \leqslant i_m \leqslant t$ dla $1 \leqslant m \leqslant p$ ($p = 0$ odpowiada ciągowi pustemu, który oznaczamy przez ε). Porządek w drzewie określamy następująco:

$$i_1 i_2 \ldots i_p \leqslant j_1 j_2 \ldots j_s \Leftrightarrow p \leqslant s \wedge i_1 = j_1 \wedge \ldots \wedge i_p = j_p.$$

Zbiór D_i elementów drzewa o randze i będzie dokładnie zbiorem tych ciągów z D, które mają długość i. Każdemu elementowi $w \in D$ przyporządkujemy pewien zbiór $S_w \subseteq X$ oraz element $x_w \in S_w$. Nasze drzewo konstruujemy indukcyjnie. Jako korzeń przyjmujemy ciąg pusty ε, przyjmujemy też $S_\varepsilon = X$, a jako x_ε przyjmujemy dowolny element zbioru X. Załóżmy, że określiliśmy już zbiór D_p elementów rangi p wraz z odpowiadającymi im zbiorami S_w i elementami x_w. Dla każdego ciągu

$w = i_1 \ldots i_p \in D_p$ oraz $1 \leqslant j \leqslant t$ wyznaczamy zbiory

$$S_{wj} = \{y \in S_w\colon \{x_w, y\} \in A_j\}$$

oraz przyjmujemy

$$D_{p+1} = \{wj\colon w \in D_p \wedge 1 \leqslant j \leqslant t \wedge S_{wj} \neq \emptyset\}.$$

Następnie dla każdego $v \in D_{p+1}$ przyjmujemy jako x_v dowolny element zbioru S_v. Zauważmy, że dla każdego $w \in D_p$

$$S_w = \{x_w\} \cup \bigcup_{j=1}^{t} S_{wj}.$$

Zatem liczność zbiorów $S_{i_1 \ldots i_p}$ maleje wraz z przedłużaniem ciągu $i_1 \ldots i_p$, i dla pewnego k otrzymamy $D_{k+1} = \emptyset$. Tak więc skonstruowane przez nas drzewo jest skończone i ma wysokość k. Łatwo zauważyć, że w trakcie konstrukcji każdy $x \in X$ zostaje w pewnym kroku wykorzystany jako x_w dla pewnego $w \in D$. Stąd $|D| = |X|$. Na mocy lematu 1.2 nasze drzewo ma wysokość $r(T) \geqslant q = \left(\sum_{i=1}^{t} (q_i - 1)\right) - t + 1$. Tak więc istnieje pewien ciąg $i_1 \ldots i_q \in D$. Odpowiada mu ciąg elementów $x_\varepsilon, x_{i_1}, x_{i_1 i_2}, \ldots, x_{i_1 \ldots i_{q-1}}, x_{i_1 \ldots i_{q-1} i_q}$. Nazwijmy, dla $p < q$, element $x_{i_1 \ldots i_p}$ tego ciągu *elementem j-tego rodzaju*, jeśli $i_{p+1} = j$. Zasada podziałowa gwarantuje nam istnienie takiego wskaźnika i ($1 \leqslant i \leqslant t$), że zbiór Z_i elementów i-tego rodzaju w naszym ciągu zawiera co najmniej $q_i - 1$ elementów. Niech $Y = Z_i \cup \{x_{i_1 \ldots i_q}\}$. Oczywiście $|Y| = q_i$. Wykażemy, że $\mathscr{P}_2(Y) \subseteq A_i$. Istotnie, jeśli $x, y \in Y$, to możemy bez zmniejszenia ogólności zakładać, że $x = x_{i_1 \ldots i_p} \in Z_i$, $y = x_{i_1 \ldots i_s}$, $s > p$. Lecz wtedy $y \in S_{i_1 \ldots i_s} \subseteq S_{i_1 \ldots i_p i_{p+1}}$, gdzie $i_{p+1} = i$, zatem, na mocy konstrukcji, $\{x, y\} \in A_i$. □

Pokazany tu drugi dowód twierdzenia Ramsey'a ma w stosunku do pierwszego dwie zalety. Po pierwsze, pozwala się łatwo uogólnić na przypadek nieskończony, o czym przekonamy się w § 10. Po drugie, daje następujące oszacowanie na liczby Ramsey'a $R_2(q_1, \ldots, q_t)$ (w dalszym ciągu zamiast $R_2(q_1, \ldots, q_t)$ będziemy pisali $R(q_1, \ldots, q_t)$):

TWIERDZENIE 1.3.

$$R(q_1, \ldots, q_t) \leqslant \frac{t^{q_1 + \ldots + q_t - 2t + 1} - 1}{t - 1} + 1. \ \square$$

W szczególności otrzymujemy $R(m, n) \leqslant \frac{1}{8} 2^{m+n}$.

§ 2. Liczby Ramsey'a

Zajmiemy się teraz bliżej wartościami liczb Ramsey'a. Pierwszym nietrywialnym przypadkiem jest $R(3, 3)$. Wykażemy, że $R(3, 3) = 6$. Istotnie, łatwo pokazać pokolorowanie krawędzi grafu K_5 na dwa kolory, przy którym nie ma trójkąta

jednego koloru (wystarczy narysować wierzchołki grafu na okręgu i pokolorować krawędzie łączącego sąsiednie wierzchołki kolorem czerwonym a wszystkie pozostałe niebieskim). Stąd $R(3, 3) > 5$. Z drugiej strony, rozważmy dowolne pokolorowanie krawędzi grafu K_6, oraz dowolny wierzchołek tego grafu. Od tego wierzchołka odchodzi 5 krawędzi, zatem jest on połączony co najmniej z trzema wierzchołkami krawędziami jednego koloru, i bez zmniejszenia ogólności możemy zakładać, że czerwonego. Jeśli co najmniej dwa spośród tych trzech wierzchołków połączone są krawędzią czerwoną, to krawędź ta „zamyka" czerwony trójkąt. W przeciwnym przypadku mamy oczywiście trójkąt niebieski. Stąd $R(3, 3) \leqslant 6$. A oto znane obecnie liczby Ramsey'a $R(m, n)$ — w przypadkach gdy dokładna wartość nie jest znana podane zostały ograniczenia dolne i górne.

n \ m	2	3	4	5	6	7	8	9
2	2	3	4	5	6	7	8	9
3		6	9	14	18	23	28/29	36
4			18	25/28	34/36			
5				42/55	57/94			
6					102/178			

Wiadomo poza tym, że $R(3, 3, 3) = 17$.

Obliczenie tak „małej" liczby Ramsey'a jak $R(5, 5)$ wydaje się już być zagadnieniem bardzo trudnym, nawet przy użyciu najszybszych dostępnych maszyn cyfrowych. Równie skromna jak nasza wiedza o asymptotycznym zachowaniu liczb $R(m, n)$ przy $m, n \to \infty$. Drugi dowód twierdzenia Ramsey'a dał nam oszacowanie $R(m, n) \leqslant \frac{1}{8} 2^{m+n}$. Okazuje się, że pierwszy dowód może też dostarczyć pewnego oszacowania. Z dowodu tego wynika mianowicie bezpośrednio następująca nierówność:

$$R_r(m, n) \leqslant R_{r-1}\big(R_r(m-1, n), R_r(m, n-1)\big)+1 \qquad (m, n > 2).$$

W szczególności dla $r = 2$ otrzymujemy

$$(2.1) \quad R(m, n) \leqslant \big(R(m-1, n)+R(m, n-1)-1\big)+1 = R(m-1, n)+R(m, n-1).$$

(Przypomnijmy, że na mocy zasady podziałowej $R_1(p, q) = p+q-1$). Mamy stąd następujące

TWIERDZENIE 2.1. *Dla dowolnych* $m, n \geqslant 2$

$$R(m, n) \leqslant \binom{m+n-2}{m-1}.$$

Dowód. Dla $m = 2$ mamy $R(m, n) = n = \binom{n}{1} = \binom{m+n-2}{m-1}$. Podobnie sprawdzamy przypadek $n = 2$. Niech teraz $m, n > 2$ i przyjmijmy jako założenie indukcyjne nierówności

$$R(m-1, n) \leqslant \binom{(m-1)+n-2}{(m-1)-1} = \binom{m+n-3}{m-2},$$

$$R(m, n-1) \leqslant \binom{m+(n-1)-2}{m-1} = \binom{m+n-3}{m-1}.$$

Mamy wtedy, wobec tożsamości (5.12) z rozdziału 1

$$R(m, n) \leqslant R(m-1, n) + R(m, n-1) \leqslant \binom{m+n-3}{m-2} + \binom{m+n-3}{m-1} = \binom{m+n-2}{m-1}. \; \square$$

Porównajmy, dla $n = m$, oszacowania $\frac{1}{8}2^{m+n} = \frac{1}{8}2^{2n}$ i $\binom{m+n-2}{m-1} = \binom{2(n-1)}{n-1}$. Na mocy wzoru Stirlinga $(n! \approx (n/e)^n \sqrt{2\pi n})$ mamy

$$\binom{2(n-1)}{n-1} \approx \frac{1}{4\sqrt{\pi(n-1)}} 2^{2n} \approx \frac{1}{4\sqrt{\pi n}} 2^{2n}$$

(p. też zad. 13), a zatem drugie oszacowanie jest asymptotycznie lepsze (przypomnijmy, że $f(n) \approx g(n)$ oznacza, iż $\lim_{n\to\infty} f(n)/g(n) = 1$). Nie jest to zresztą najlepsze znane oszacowanie: wiadomo, że dla pewnej stałej c i dowolnych $n \geqslant m \geqslant 3$

$$R(m, n) \leqslant c \frac{\log \log n}{\log n} \binom{m+n-2}{m-1}$$

(J. Yackel [1]).(¹)

Przejdziemy teraz do oszacowań dolnych dla liczb Ramsey'a. Udowodnimy najpierw ogólne twierdzenie, które może być również pomocne do otrzymania ograniczeń dolnych na odpowiedniki liczb Ramsey'a dla innych twierdzeń podziałowych. Będziemy mówili, że rodzina $\mathscr{X} \subseteq \mathscr{P}_n(X)$ jest *dwukolorowalna*, jeśli elementy zbioru X można pokolorować dwoma kolorami tak, by żaden podzbiór $A \in \mathscr{X}$ nie składał się z elementów tego samego koloru. Innymi słowy rodzina $\mathscr{X}$ jest dwukolorowalna, jeśli istnieje podzbiór $C \subseteq X$ taki, że $\emptyset \subsetneq A \cap C \subsetneq A$ dla każdego $A \in \mathscr{X}$.

TWIERDZENIE 2.2. *Niech X będzie dowolnym zbiorem skończonym, $n \geqslant 1$, $\mathscr{X} \subseteq \mathscr{P}_n(X)$. Jeśli $\mathscr{X}$ nie jest dwukolorowalna, to $|\mathscr{X}| \geqslant 2^{n-1}$.*

Dowód. Niech $|X| = m$. Obliczymy na dwa sposoby liczbę par $\langle A, C\rangle$ takich, że $A \in \mathscr{X}$ oraz $A \subseteq C$ lub $A \subseteq X \setminus C$. Każdemu zbiorowi $A \in \mathscr{X}$ odpowiada 2^{m-n}

(¹) Prawdziwość tego oszacowania jest kwestionowana, p. Chung [1].

zbiorów $C \supseteq A$ oraz 2^{m-n} zbiorów C takich, że $X \setminus C \supseteq A$. Zatem naszych par jest $|\mathscr{X}| 2^{m-n+1}$. Z drugiej strony, na mocy założenia, każdemu zbiorowi $C \subseteq X$ odpowiada co najmniej jeden zbiór $A \in \mathscr{X}$ taki, że $A \subseteq C$ lub $A \subseteq X \setminus C$. Stąd naszych par jest co najmniej tyle co zbiorów $C \subseteq X$. Mamy więc

$$|\mathscr{X}| 2^{m-n+1} \geqslant 2^m,$$

czyli

$$|\mathscr{X}| \geqslant 2^{n-1}. \ \square$$

Można też wykazać, że $|\mathscr{X}| \geqslant 2^n n/(n+2)$. Zainteresowanego Czytelnika odsyłamy do oryginalnej pracy Schmidta [2] lub do monografii Erdösa i Spencera [1].

Aby otrzymać dolne oszacowanie liczb Ramsey'a, wystarczy teraz odpowiednio dobrać rodzinę $\mathscr{X}$. Jeśli mianowicie rozważymy zbiór X o liczności $m = R(n, n)$ oraz przyjmiemy $\mathscr{X} = \{\mathscr{P}_2(Y)\colon Y \in \mathscr{P}_n(X)\}$, to z definicji $R(n, n)$ rodzina $\mathscr{X}$ nie jest dwukolorowalna. Lecz $\mathscr{X} \subseteq \mathscr{P}_{\binom{n}{2}}(\mathscr{P}_2(X))$ oraz $|\mathscr{X}| = \binom{m}{n}$. Otrzymujemy stąd jako wniosek następujące*

Twierdzenie 2.3 (Erdös [2]).

$$R(n, n) \geqslant n 2^{n/2} \left(\frac{1}{e\sqrt{2}} - o(1) \right).$$

Dowód. Z twierdzenia 2.2 otrzymujemy

$$\binom{m}{n} \geqslant 2^{\binom{n}{2} - 1}.$$

Lecz

$$\binom{m}{n} = \frac{m(m-1)\,\ldots\,(m-n+1)}{n(n-1)\,\ldots\,1} \leqslant \frac{m^n}{n!}.$$

Stąd

$$m^n \geqslant n!\, 2^{(n^2-n-2)/2},$$

$$m \geqslant \sqrt[n]{n!}\, 2^{n/2} 2^{-1/2} 2^{-1/n} \approx \sqrt[n]{n!}\, \frac{1}{\sqrt{2}} 2^{n/2} \approx n 2^{n/2} \frac{1}{e\sqrt{2}},$$

gdyż na mocy wzoru Stirlinga mamy

$$\sqrt[n]{n!} \approx \frac{n}{e} \sqrt[2n]{2n}\, \sqrt[2n]{\pi} \approx \frac{n}{e}. \ \square$$

Porównując otrzymane w tym paragrafie dolne i górne ograniczenia liczb Ramsey'a $R(n, n)$ widzimy, jak mało jeszcze wiemy o szybkości wzrostu tych liczb

* Przypomnijmy, że symbol $o(1)$ oznacza funkcję (zmniennej n) zbieżną do zera (dla $n \to \infty$).

przy $n \to \infty$. Twierdzenie 2.2 zostało opublikowane przez Erdősa w 1947 r. i dotychczas nikomu nie udało się podać istotnie lepszego oszacowania dolnego (jeśli nie liczyć pracy Spencera [2] zwiększającej to ograniczenie dwukrotnie).

Dodatkowe informacje dotyczące oszacowań na liczby Ramsey'a można znaleźć w pracach Ajtai, Komlós i Szemerédi [1], Griggs [1], Abbott i Liu [2], Nara i Tachibana [1] oraz Chung [1].

§ 3. Twierdzenia podziałowe dla grafów

Omawiając twierdzenie Ramsey'a (dla $r = 2$) wspomnieliśmy o jego następującej teoriografowej interpretacji: Jeśli $m \geqslant R(p, q)$, to przy dowolnym pokolorowaniu krawędzi grafu K_m na czerwono lub niebiesko powstaje podgraf izomorficzny z K_p o wszystkich krawędziach czerwonych lub podgraf izomorficzny z K_q o wszystkich krawędziach niebieskich (przypomnijmy, że K_m oznacza graf pełny o m wierzchołkach). Problem ten możemy w naturalny sposób uogólnić: Dla danych grafów G, H szukamy najmniejszej liczby $r(G, H)$ takiej, że dla dowolnego $m \geqslant r(G, H)$ przy dowolnym pokolorowaniu krawędzi grafu K_m kolorami czerwonym i niebieskim powstaje podgraf izomorficzny z G o wszystkich krawędziach czerwonych lub też podgraf izomorficzny z H o wszystkich krawędziach niebieskich. Oczywiście $R(p, q) = r(K_p, K_q)$ natomiast istnienie liczb $r(G, H)$ dla dowolnych G, H jest oczywistym wnioskiem z twierdzenia Ramsey'a: jeśli G i H mają odpowiednio p i q wierzchołków, to $r(G, H) \leqslant R(p, q)$. Nietrywialny jest natomiast problem wyznaczania liczb $r(G, H)$ dla konkretnych grafów G, H. Zainteresowanego Czytelnika odsyłamy do bogatej literatury na ten temat (p. np. Burr [1]), my zaś zajmiemy się pewną modyfikacją tego problemu. Przez podgraf grafu $G = \langle V, E \rangle$ o zbiorze wierzchołków V i zbiorze krawędzi $E \subseteq \mathscr{P}_2(V)$ rozumieliśmy dowolny graf $G_1 = \langle V_1, E_1 \rangle$ taki, że $V_1 \subseteq V$, $E_1 \subseteq E$. Przypomnijmy, że podgraf taki nazywamy podgrafem indukowanym przez zbiór V_1 (i oznaczamy przez G_{V_1}), jeśli $E_1 = E \cap \mathscr{P}_2(V_1)$, tzn. jeśli G_1 zawiera wszystkie krawędzie grafu G łączące wierzchołki ze zbioru V_1. Przez podgraf indukowany będziemy rozumieli podgraf indukowany przez swój zbiór wierzchołków. Głównym rezultatem w tym paragrafie będzie następujące

TWIERDZENIE 3.1 (Deuber [2]). *Dla dowolnych grafów G i H istnieje graf L o następującej własności:*

Dla każdego pokolorowania krawędzi grafu L na dwa kolory, czerwony i niebieski, istnieje w L podgraf indukowany o wszystkich krawędziach czerwonych izomorficzny z G, lub podgraf indukowany o wszystkich krawędziach niebieskich izomorficzny z H.

Dowód. Niech $L \to (G, H)$ oznacza własność grafu L, o której mowa w tezie twierdzenia, i niech zbiorami wierzchołków grafów G i H będą odpowiednio $X = V(G)$ i $Y = V(H)$. Będziemy dowodzili twierdzenia przez indukcję względem $|X| + |Y|$. Dla „małych" grafów G, H twierdzenie jest oczywiste: jeśli $|X| = 1$ lub

$|Y| = 1$, to $L \to (G, H)$ dla dowolnego grafu L. Niech więc $|X| > 1$ i $|Y| > 1$. Ustalmy $x \in X$, $y \in Y$ i rozważmy grafy $\bar{G} = G_{X \setminus \{x\}}$, $\bar{H} = H_{Y \setminus \{y\}}$. Na mocy założenia indukcyjnego istnieją grafy G^* i H^* takie, że $G^* \to (\bar{G}, H)$ oraz $H^* \to (G, \bar{H})$. Niech $\bar{G}_1, \bar{G}_2, \ldots, \bar{G}_m$ będą wszystkimi podgrafami indukowanymi grafu G^* izomorficznymi z $\bar{G}$. Istnieją wtedy zbiory $S_1, S_2, \ldots, S_m$ takie, że $S_i \subseteq V(\bar{G}_i)$, i jeśli do $\bar{G}_i$ dodamy „nowy" wierzchołek (tzn. nie będący wierzchołkiem grafu G^*) i połączymy go z wszystkimi wierzchołkami z S_i, to otrzymamy graf izomorficzny z G (zauważmy, że zbiór S_i nie musi być jednoznacznie wyznaczany przez $\bar{G}_i$). Konstrukcji żądanego grafu L dokonamy w m krokach, startując od G.

Niech $L_0 = G^*$, niech $\{x_1, \ldots, x_l\}$ będzie zbiorem wierzchołków grafu G^* i niech $X_i^0 = \{x_i\}$ dla $1 \leqslant i \leqslant l$ (X_i^j jest zbiorem wierzchołków powstałych z x_i w trakcie pierwszych j kroków naszej konstrukcji). Przy założeniu, że określiliśmy już graf L_{j-1} oraz zbiory $X_i^{j-1} \subseteq V(L_{j-1})$, skonstruujemy graf L_j i zbiory $X_i^j \subseteq V(L_j)$ $(1 \leqslant j \leqslant m,\ 1 \leqslant i \leqslant l)$. W tym celu zdefiniujmy

$$Z_j = \bigcup \{X_i^{j-1}\colon\ x_i \in S_j\} \subseteq V(L_{j-1}),$$

oraz zamieńmy kolejno każdy wierzchołek $z \in Z_j$ na kopię H_z^* grafu H^* (każdy wierzchołek z $V(H_z^*)$ jest połączony ze wszystkimi wierzchołkami, z którymi połączony był z). Dokładniej, definiujemy najpierw pomocniczy graf L'_j następująco:

$$V(L'_j) = \big(V(L_{j-1}) \setminus Z_j\big) \cup \big(Z_j \times V(H^*)\big),$$

$$\begin{aligned} E(L'_j) = &\ \{\{x, y\} \in E(L_{j-1})\colon\ x, y \notin Z_j\} \cup \\ &\cup \{\{x, \langle z, y\rangle\}\colon\ \{x, z\} \in E(L_{j-1}) \wedge x \notin Z_j \wedge z \in Z_j \wedge y \in V(H^*)\} \cup \\ &\cup \{\{\langle u, x\rangle, \langle v, y\rangle\}\colon\ u, v \in Z_j \wedge x, y \in V(H^*) \wedge \{u, v\} \in E(L_{j-1})\} \cup \\ &\cup \{\{\langle u, x\rangle, \langle u, y\rangle\}\colon\ u \in Z_j \wedge \{x, y\} \in E(H^*)\}. \end{aligned}$$

Każda z kopii H_z^* grafu H^* zawiera pewną liczbę podgrafów indukowanych $\bar{H}_z^1, \bar{H}_z^2, \ldots, \bar{H}_z^n$ izomorficznych z $\bar{H}$. Istnieje dla każdego z nich zbiór $T_z^i \subseteq V(\bar{H}_z^i)$ wierzchołków, które należy połączyć z nowym wierzchołkiem, by otrzymać graf izomorficzny z H. Możemy na $n^{|Z_j|}$ sposobów wybrać po jednym zbiorze T_z^i z każdego grafu H_z^* $(z \in Z_j,\ 1 \leqslant i \leqslant n)$. Dla każdego takiego wyboru $T_{z_1}^{i_1}, T_{z_2}^{i_2}, \ldots, T_{z_q}^{i_q}$ $(Z_j = \{z_1, \ldots, z_q\},\ 1 \leqslant i_p \leqslant n$ dla $1 \leqslant p \leqslant q)$ dodajemy do L'_j nowy wierzchołek $z^j_{i_1 i_2 \ldots i_q}$, który łączymy ze wszystkimi wierzchołkami ze zbioru $\bigcup_{p=1}^{q} T_{z_p}^{i_p}$. Otrzymujemy w ten sposób graf L_j. Pozostaje jeszcze określić zbiory X_i^j. Definiujemy

$$X_i^j = \begin{cases} X_i^{j-1}, & \text{jeśli } x_i \notin S_j, \\ X_i^{j-1} \times V(H^*), & \text{jeśli } x_i \in S_j. \end{cases}$$

Jak już wspomnieliśmy, X_i^j jest zbiorem tych wierzchołków grafu L_j, które powstały z x_i w procesie (na ogół wielokrotnego) „rozszczepiania" tego wierzchołka

(przy zamianie wierzchołka na kopię grafu H^*, wierzchołek ten „rozszczepia się" na $|V(H^*)|$ wierzchołków kopii).

Przyjmujemy $L = L_m$. Należy teraz sprawdzić, że $L \to (G, H)$. W tym celu załóżmy, że każdą z krawędzi grafu L_m pokolorowaliśmy na czerwono lub niebiesko tak, że nie powstał żaden podgraf indukowany o wszystkich krawędziach czerwonych izomorficzny z G, ani też żaden podgraf indukowany o wszystkich krawędziach niebieskich izomorficzny z H. Wykażemy, iż założenie to prowadzi do sprzeczności. Istotnie, w każdym z podgrafów $H^*_{z_p}$, $z_p \in Z_m$, musi wtedy istnieć podgraf indukowany $H^{i_p}_{z_p}$ izomorficzny z $\bar{H}$ o wszystkich krawędziach niebieskich. Zbiorom $T^{i_p}_{z_p} \subseteq V(\bar{H}^{i_p}_{z_p})$ odpowiada pewien wierzchołek $z^m_{i_1 i_2 \ldots i_s}$ $(s = |Z_m|)$. Wierzchołek ten musi być połączony z każdym ze zbiorów $T^{i_p}_{z_p}$ co najmniej jedną krawędzią czerwoną (w przeciwnym przypadku powstałby „niebieski" podgraf indukowany izomorficzny z H). Wybieramy z każdego zbioru $T^{i_p}_{z_p}$ po jednym wierzchołku t_p połączonym z $z^m_{i_1 i_2 \ldots i_s}$ krawędzią czerwoną. Usuwamy pozostałe elementy zbiorów $V(H^*_{z_p})$ wraz z incydentnymi z nimi krawędziami. Usuwamy również wszystkie wierzchołki $z^m_{j_1 j_2 \ldots j_s}$ różne od $z^m_{i_1 i_2 \ldots i_s}$, wraz z incydentnymi z nimi krawędziami. Otrzymany w ten sposób graf jest izomorficzny z L_{m-1} z dodanym wierzchołkiem połączonym czerwonymi krawędziami ze wszystkimi wierzchołkami ze zbioru $\bigcup \{X^{m-1}_i \colon x_i \in S_m\}$, tzn. ze wszystkimi wierzchołkami grafu L_{m-1} powstałymi z rozszczepienia wierzchołków z S_m. Zauważmy, że istotą dokonanej przed chwilą konstrukcji jest powrót od L_m do L_{m-1}: odpowiednie kopie grafu H^* zamienialiśmy na pojedyncze wierzchołki. Konstrukcję tę powtarzamy, otrzymując graf izomorficzny z L_{m-2} z dodanymi dwoma wierzchołkami: jednym połączonym czerwonymi krawędziami z wszystkimi wierzchołkami powstałymi z rozszczepienia wierzchołków z S_m i drugim połączonym czerwonymi krawędziami z wszystkimi wierzchołkami powstałymi z rozszczepienia wierzchołków z S_{m-1}. Powtarzając tę konstrukcję otrzymujemy w końcu graf L_0^+ izomorficzny z $L_0 = G^*$ z dodanymi, dla $1 \leqslant i \leqslant m$, wierzchołkami u_i połączonymi czerwonymi krawędziami ze wszystkimi wierzchołkami z S_i. Lecz $G^* \to (\bar{G}, H)$, zatem musi być w G^* albo „czerwony" podgraf indukowany izomorficzny z $\bar{G}$, który wraz z pewnym wierzchołkiem u_i i incydentnymi z nimi krawędziami tworzy „czerwony" podgraf indukowany grafu L_0^+ izomorficzny z G, albo „niebieski" podgraf indukowany izomorficzny z H. Lecz w obu przypadkach podgrafy te są podgrafami indukowanymi grafu L_m (gdyż L_0, L_0^+ są podgrafami indukowanymi grafu L_m). Otrzymaliśmy sprzeczność z założeniem, iż przy naszym pokolorowaniu grafu L_m nie ma w L_m ani „czerwonego" podgrafu indukowanego izomorficznego z G, ani „niebieskiego" podgrafu indukowanego izomorficznego z H. Sprzeczność ta kończy dowód. □

Na zakończenie warto wspomnieć, że twierdzenie Deubera zostało wzmocnione przez Nešetřila i Rödla [1] w następujący sposób: Dla dowolnych grafów G i H istnieje graf L taki, że $L \to (G, H)$ oraz $\omega(L) = \max\{\omega(G), \omega(H)\}$, gdzie $\omega(G)$ jest maksymalną licznością kliki w G (por. rozdział 4, § 2).

§ 4. Twierdzenie van der Waerdena

Przechodzimy do własności podziałowych zbioru liczb naturalnych. W paragrafie tym wykażemy, że dla dowolnych k, t można dobrać m tak duże, że ilekroć $\{1, \ldots, m\} = A_1 \cup \ldots \cup A_t$, to któryś ze zbiorów A_i zawiera postęp arytmetyczny długości k. W następnym paragrafie udowodnimy, że dla dostatecznie dużego m (zależnego od n) i dowolnego podziału $\{1, \ldots, m\} = A_1 \cup \ldots \cup A_n$ któryś ze zbiorów A_i zawiera liczby x_1, x_2, x_3 (niekoniecznie różne) takie, że $x_1 + x_2 = x_3$. Oba te problemy są, jak widać, zagadnieniami addytywnej teorii liczb.

TWIERDZENIE 4.1 (van der Waerden [1]). *Dla dowolnych $k, t \in N$ istnieje liczba n o następującej własności:*

Dla dowolnego $m \geqslant n$ i dowolnego podziału $\{1, \ldots, m\} = A_1 \cup \ldots \cup A_t$ istnieje $i \in \{1, \ldots, t\}$ takie, że zbiór A_i zawiera postęp arytmetyczny długości k.

Najmniejszą z liczb n o powyższej własności będziemy oznaczali przez $W(t, k)$.

Dowód (p. Graham i Rotschild [2]). Wygodnie nam będzie reprezentować dowolny podział $X = X_1 \dot{\cup} \ldots \dot{\cup} X_t$ przez funkcję $C\colon X \to \{1, \ldots, t\}$ taką, że $X_i = \{x \in X\colon C(x) = i\}$. Możemy sobie wyobrażać, że funkcja C przyporządkowuje każdemu $x \in X$ jego „kolor” $C(x) \in \{1, \ldots, t\}$. Będziemy mówili, że dla dowolnego r dwa ciągi $\langle x_1, \ldots, x_r\rangle$, $\langle y_1, \ldots, y_r\rangle \in \{0, \ldots, k\}^r$ są *k-równoważne*, jeśli pokrywają się one do ostatniego wystąpienia liczby k, tzn. jeśli istnieje $p \in \{0, \ldots, r\}$ takie, że $x_i = y_i$ dla $i \leqslant p$ oraz $x_i \neq k$, $y_i \neq k$ dla $i > p$ (piszemy wtedy $\langle x_1, \ldots, x_r\rangle \underset{k}{\equiv} \langle y_1, \ldots, y_r\rangle$). Jest oczywiste, że $\underset{k}{\equiv}$ jest relacją równoważności. Dla dowolnych $k, r \in N$ niech $S(k, r)$ oznacza zdanie:

Dla każdego $t \geqslant 1$ istnieje liczba $N(k, r, t)$ taka, że dla dowolnej funkcji $C\colon \{1, \ldots, N(k, r, t)\} \to \{1, \ldots, t\}$ istnieją $a, d_1, \ldots, d_r > 0$ takie, że wyrażenie $C(a + \sum_{i=1}^{r} x_i d_i)$ jest stałe na każdej klasie równoważności $\underset{k}{\equiv}$ określonej na zbiorze $\{0, \ldots, k\}^r$ (tzn. $C(a + \sum_{i=1}^{r} x_i d_i) = C(a + \sum_{i=1}^{r} y_i d_i)$ dla dowolnych $\langle x_1, \ldots, x_r\rangle \underset{k}{\equiv} \langle y_1, \ldots, y_r\rangle$).

Udowodnimy $S(k, r)$ dla dowolnych $k, r \geqslant 1$. Twierdzenie van der Waerdena otrzymamy stąd jako wniosek, gdyż jest to dokładnie $S(k, 1)$ dla każdego $k \geqslant 1$. Istotnie, dla $r = 1$ mamy dokładnie 2 klasy k-równoważności: jedną złożoną z ciągów (długości 1) $\langle 0\rangle, \langle 1\rangle, \ldots, \langle k-1\rangle$ oraz drugą złożoną z ciągu $\langle k\rangle$. Tak więc $S(k, 1)$ orzeka, iż przy odpowiednich założeniach liczby $a + jd$, $0 \leqslant j \leqslant k-1$ są tego samego koloru dla pewnych $a, d > 0$.

$S(k, r)$ dowodzimy przez indukcję względem par $\langle k, r\rangle$ uporządkowanych leksykograficznie:

$$\langle k', r'\rangle \leqslant \langle k, r\rangle \Leftrightarrow k' < k \vee (k' = k \wedge r' \leqslant r).$$

Zdanie $S(1, 1)$ jest w trywialny sposób prawdziwe. Wystarczy teraz udowodnić, że $S(k, r) \Rightarrow S(k, r+1)$, i że jeśli $S(k, r)$ dla wszystkich $r \geqslant 1$, to $S(k+1, 1)$.

$S(k, r) \Rightarrow S(k, r+1)$. Niech dla pewnego ustalonego t $M = N(k, r, t)$ i M'

$= N(k, 1, t^M)$ (istnienie tej ostatniej liczby jest oczywistym wnioskiem z $S(k, r)$). Wykażemy, że MM' możemy przyjąć jako $N(k, r+1, t)$. Istotnie, niech będzie dane „pokolorowanie" C: $\{1, \ldots, MM'\} \to \{1, \ldots, t\}$. Odcinek $\{1, \ldots, MM'\}$ możemy sobie wyobrażać jako M' następujących po sobie bloków długości M. Każdy z tych bloków może być pokolorowany przez C na jeden spośród t^M „wzorów". Zdefiniujmy funkcję C': $\{1, \ldots, M'\} \to \{1, \ldots, t^M\}$ tak, by $C'(i) = C'(j)$ wtedy i tylko wtedy, gdy i-ty i j-ty blok są pokolorowane na ten sam wzór, tzn. gdy $C(iM-p) = C(jM-p)$ dla $0 \leqslant p \leqslant M-1$. Na mocy definicji liczby M' istnieją $a', d' > 0$ takie, że $C'(a'+jd')$ jest stałe dla $j \in \{0, \ldots, k-1\}$. $S(k, r)$ możemy również zastosować do odcinka $\{(a'-1)M+1, \ldots, a'M\}$, zatem na mocy definicji liczby M istnieją $a, d_1, \ldots, d_r > 0$ takie, że $(a'-1)M+1 \leqslant a+\sum x_i d_i \leqslant a'M$ oraz wyrażenie $C(a+\sum_{i=1}^{r} x_i d_i)$ jest stałe na każdej klasie równoważności relacji $\underset{k}{\equiv}$. Przyjmijmy teraz $d_i' = d_i$ dla $1 \leqslant i \leqslant r$ oraz $d_{r+1}' = d'M$, i niech

$$p = C(a+\sum_{i=1}^{r+1} x_i d_i'), \qquad q = C(a+\sum_{i=1}^{r+1} y_i d_i'),$$

gdzie $\langle x_1, \ldots, x_{r+1}\rangle \underset{k}{\equiv} \langle y_1, \ldots, y_{r+1}\rangle$. Jeśli $x_{r+1} = k$, to $\langle x_1, \ldots, x_{r+1}\rangle = \langle y_1, \ldots, y_{r+1}\rangle$ i oczywiście $p = q$. Niech więc $x_{r+1}, y_{r+1} < k$. Wobec $\langle x_1, \ldots, x_r\rangle \underset{k}{\equiv} \langle y_1, \ldots, y_r\rangle$ liczby $a+\sum_{i=1}^{r} x_i d_i'$, $a+\sum_{i=1}^{r} y_i d_i'$ są tego samego koloru. Lecz dodając do nich odpowiednio $x_{i+1}d_{i+1}' = x_{i+1}d'M$ i $y_{i+1}d_{i+1} = y_{i+1}d'M$ nie zmieniamy ich koloru, gdyż przesuwamy się do identycznie pokolorowanych bloków. Tak więc i w tym przypadku $p = q$. Zatem wyrażenie $C(a+\sum_{i=1}^{r+1} x_i d_i')$ jest stałe na każdej klasie równoważności $\underset{k}{\equiv}$. Ponieważ t było dowolne, przeto udowodniliśmy $S(k, r+1)$.

$S(k, r)$ dla wszystkich $r \geqslant 1 \Rightarrow S(k+1, 1)$. Niech dla pewnego ustalonego $t \geqslant 1$ będzie dane pokolorowanie C: $\{1, \ldots, 2N(k, t, t)\} \to \{1, \ldots, t\}$. Istnieją wtedy a, $d_1, \ldots, d_t > 0$ takie, że dla dowolnych $\langle x_1, \ldots, x_t\rangle \in \{0, \ldots, k\}^t$ mamy $a+\sum_{i=1}^{t} x_i d_i \leqslant N(k, t, t)$ oraz wyrażenie $C(a+\sum_{i=1}^{t} x_i d_i)$ jest stałe na każdej klasie równoważności $\underset{k}{\equiv}$. Na mocy zasady szufladkowej Dirichleta istnieją wśród liczb $a+\sum_{i=1}^{p} kd_i$, $0 \leqslant p \leqslant t$ dwie tego samego koloru, powiedzmy $a+\sum_{i=1}^{u} kd_i$ oraz $a+\sum_{i=1}^{v} kd_i$ $(u < v)$. Stąd $C((a+\sum_{i=1}^{u} kd_i)+j\sum_{i=u+1}^{v} d_i)$ jest stałe dla $0 \leqslant j \leqslant k$, gdyż

$$\langle \underbrace{k, \ldots, k}_{u}, \underbrace{j, \ldots, j}_{v-u}, \underbrace{0, \ldots, 0}_{t-v}\rangle, \qquad 0 \leqslant j \leqslant k-1,$$

są w jednej klasie równoważności $\underset{k}{\equiv}$. Tak więc $N(k+1, 1, t) \leqslant 2N(k, t, t)$, i wobec dowolności t udowodniliśmy $S(k+1, 1)$.

Zauważmy jeszcze, że funkcję C określiliśmy na zbiorze $\{1, \ldots, 2N(k, t, t)\}$ tylko dlatego, iż definicja liczby $N(k+1, 1, t)$ wymagała określoności funkcji C dla argumentu $(a+\sum_{i=1}^{u} kd_i)+(k+1)\sum_{i=u+1}^{v} d_i$. □

Inne dowody twierdzenia van der Waerdena można znaleźć w pracach Deubera [3], Taylora [1] i Millsa [1].

Jako wniosek otrzymujemy

TWIERDZENIE 4.2 (van der Waerden [1]). *Dla dowolnego t, jeśli $N = A_1 \dot\cup \ldots \dot\cup A_t$, to dla pewnego $i \in \{1, \ldots, t\}$ zbiór A_i zawiera postępy arytmetyczne dowolnej długości.*

Dowód. Niech $Z_i = \{k\colon A_i$ zawiera postęp arytmetyczny długości $k\}$, $1 \leqslant i \leqslant t$. Na mocy twierdzenia 4.1 każda liczba k należy do pewnego zbioru A_i (albowiem nasz podział indukuje podział $\{1, \ldots, W(t, k)\} = B_1 \dot\cup \ldots \dot\cup B_t$, $B_i = A_i \cap \{1, \ldots, W(t, k)\}$). Innymi słowy: $Z_1 \cup \ldots \cup Z_t = N$. Co najmniej jeden ze zbiorów – powiedzmy Z_i – jest nieskończony, a więc zawiera dowolnie duże liczby naturalne. Lecz Z_i zawierając pewną liczbę zawiera wszystkie liczby od niej mniejsze. Stąd $Z_i = N$. □

Inny dowód twierdzenia van der Waerdena, a także pewne jego wzmocnienie, poznamy w § 7.

Warto tu wspomnieć, że Szemerédi [1] wzmocnił twierdzenie van der Waerdena w następujący sposób: Jeśli pewien zbiór $R \subseteq N$ spełnia warunek

$$\overline{\lim_{n\to\infty}} \frac{|R \cap \{1, \ldots, n\}|}{n} > 0,$$

to R zawiera postępy arytmetyczne dowolnej długości. Dowód tego faktu jest jednak niezwykle skomplikowany.

Na podobieństwo liczb Ramsey'a zdefiniujmy $w(k_1, \ldots, k_t)$ jako najmniejszą liczbę m o tej własności, że ilekroć $\{1, \ldots, m\} = A_1 \cup \ldots \cup A_t$, to istnieje $i \in \{1, \ldots, t\}$ takie, że A_i zawiera postęp arytmetyczny długości k_i. Jeśli $k_1 = \ldots = k_t = k$, to oczywiście $w(k_1, \ldots, k_t) = W(t, k)$. Liczby $w(k_1, \ldots, k_t)$ nazywamy *liczbami van der Waerdena.* Nasza wiedza dotycząca ich dokładnych wartości oraz asymptotycznego zachowania się przy wzroście $t, k_1, \ldots, k_t$ jest równie skąpa jak w przypadku liczb Ramsey'a. Poniższa tablica przedstawia niektóre znane wartości liczb $w(k, l)$ (oczywiście $w(k, l) = w(l, k)$).

k \ l	2	3	4	5	6	7	8	9	10
2	3	6	7	10	11	14	15	18	19
3		9	18	22	32	46	58	77	97
4			35	55	73	109			
5				178					

Znane są też liczby $w(3, 3, 3) = 27$, $w(3, 3, 4) = 51$, $w(3, 3, 3, 3) = 76$ (por. Beeler i O'Neil [1]). Znalezienie tej ostatniej wartości zajęło 1200 godzin pracy komputera.

Oszacowania górne dla liczb van der Waerdena wynikające ze znanych dowodów twierdzenia van der Waerdena rosną tak szybko ze wzrostem t i k, że nie dają się nawet wyrazić w zwartej postaci analitycznej. Wydaje się, że mają one niewiele wspólnego z prawdziwą szybkością wzrostu liczb van der Waerdena.

Istnieje bogata literatura dotycząca dolnych oszacowań dla $W(t, k)$. Erdös i Rado [1] wykazali, że

$$W(t, k) > (2(k-1)t^{k-1})^{1/2}$$

(zakładamy tu, podobnie jak we wszystkich poniższych oszacowaniach, $t \geqslant 2$, $k \geqslant 3$). Schmidt [1] poprawił to oszacowanie do

$$W(t, k) \geqslant t^{k - c(k \log k)^{1/2}}$$

dla pewnej stałej c. Dla k małego w porównaniu z t lepsze jest oszacowanie L. Mosera [1]:

$$W(t, k) > (k-1)t^{c \log t},$$

lub Abbotta i Liu [1]:

$$W(t, k) > t^{c(s)(\log t)^s}, \qquad s = \lfloor \log(k-1) \rfloor,$$

gdzie $c(s)$ zależy jedynie od s. Wszystkie te oszacowania, oprócz oszacowania Mosera, zostały wyprowadzone metodami niekonstruktywnymi, tzn. bez pokazywania konkretnych podziałów o blokach bez długich postępów arytmetycznych. Berlekamp [1] uzyskał metodami konstruktywnymi, wykorzystując własności ciał skończonych, oszacowanie

$$W(t, k) > \min_{\delta \in \Delta} \{(k-1)(t^{k-1} - 1)/\delta\},$$

gdzie Δ jest zbiorem wszystkich liczb naturalnych postaci $k^d - 1$, gdzie d jest dzielnikiem właściwym liczby $k-1$, lub też postaci D, gdzie D jest dowolnym dzielnikiem liczby $t^{k-1} - 1$ i $D < k-1$. Podał on również oszacowanie

$$W(2, k) > (k-1)2^{k-1}$$

dla przypadku, gdy $k-1$ jest liczbą pierwszą.

Na zakończenie tego paragrafu podamy pewne ogólne twierdzenie pozwalające wnioskować o niektórych własnościach podziałowych zbiorów skończonych na podstawie własności podziałowych odpowiednich zbiorów nieskończonych. Twierdzenie to umożliwia w szczególności proste wyprowadzenie twierdzenia 4.1 z twierdzenia 4.2. Wprowadzimy najpierw pewną ogólną terminologię dotyczącą własności podziałowych. Będziemy mówili, że rodzina zbiorów $\mathscr{F}$ jest *t-regularna* w zbiorze X, jeśli dla dowolnego podziału $X = X_1 \dot{\cup} \ldots \dot{\cup} X_t$ istnieje $i \in \{1, \ldots, t\}$

oraz zbiór $F \in \mathscr{F}$ taki, że $F \subseteq X_i$. W tej terminologii twierdzenie Ramsey'a orzeką, iż jeśli $|A| \geqslant R_r(q_1, \ldots, q_t)$, $q_1 = \ldots = q_t = q$, to rodzina $\{\mathscr{P}_r(Z)\colon Z \in \mathscr{P}_q(A)\}$ jest t-regularna w $\mathscr{P}_r(A)$, natomiast twierdzenie 4.2 mówi, że dla dowolnych k i t zbiór wszystkich postępów arytmetycznych długości k jest t-regularny w N.

TWIERDZENIE 4.3. *Jeśli $\mathscr{F}$ jest dowolną rodziną zbiorów skończonych, to $\mathscr{F}$ jest t-regularna w X wtedy i tylko wtedy, gdy jest t-regularna w pewnym skończonym podzbiorze $Y \subseteq X$.*

Dowód. Jeśli $\mathscr{F}$ jest t-regularna w pewnym zbiorze Y, to jest oczywiście t-regularna w każdym zbiorze $X \supseteq Y$. Do dowodu twierdzenia wystarczy więc wykazać, że jeśli $\mathscr{F}$ nie jest t-regularna w żadnym $Y \subseteq_{\text{fin}} X$, to nie jest t-regularna w X.

Zamiast o podziałach $X = X_1 \dot\cup \ldots \dot\cup X_t$ będziemy mówili o odpowiednich „pokolorowaniach" $C\colon X \to \{1, \ldots, t\}$. Załóżmy, że dla dowolnego $Y \subseteq_{\text{fin}} X$ istnieje pokolorowanie $C_Y\colon Y \to \{1, \ldots, t\}$, przy którym żaden zbiór $F \in \mathscr{F}$ nie jest jednokolorowy. Na mocy zasady selekcji Rado (p. rozdział 1, twierdzenie 12.1) istnieje „globalne" pokolorowanie $C\colon X \to \{1, \ldots, t\}$ o tej własności, że dla każdego $Z \subseteq_{\text{fin}} X$ istnieje zbiór $Y \subseteq_{\text{fin}} X$ taki, że $Z \subseteq Y$ oraz $C \upharpoonright Z = C_Y \upharpoonright Z$. W szczególności oznacza to, iż pokolorowanie dowolnego $F \in \mathscr{F}$ przez C pokrywa się z „lokalnym" pokolorowaniem tego zbioru przez C_Y dla pewnego $Y \supseteq F$, i w konsekwencji przy pokolorowaniu C żaden ze zbiorów $F \in \mathscr{F}$ nie jest jednokolorowy. Tak więc rodzina $\mathscr{F}$ nie jest t-regularna w X. □

Warto zwrócić uwagę na niekonstruktywny charakter tego twierdzenia: wnioskując o istnieniu odpowiedniego zbioru $Y \subseteq_{\text{fin}} X$ nie otrzymujemy żadnej informacji jak taki zbiór skonstruować, ani też żadnego oszacowania jego liczności.

§ 5. Zbiory wolne od sum i twierdzenie Schura

Będziemy mówili, że zbiór X złożony z liczb naturalnych (przypomnijmy, że 0 nie uważamy za liczbę naturalną) *jest wolny od sum*, jeśli $x+y \notin X$ dla dowolnych $x, y \in X$ (czyli równoważnie: jeśli $x-y \notin X$ dla dowolnych $x, y \in X$).

TWIERDZENIE 5.1 (Schur [1]). *Jeśli $m \geqslant \lfloor n!e \rfloor$, to dla dowolnego podziału $\{1, \ldots, m\} = X_1 \dot\cup \ldots \dot\cup X_n$ istnieje $i \in \{1, \ldots, n\}$ takie, że zbiór X_i nie jest wolny od sum*.*

Dowód. Niech $\{1, \ldots, m\} = X_1 \dot\cup \ldots \dot\cup X_n$, gdzie wszystkie zbiory X_i są wolne od sum. Wykażemy, że $m \leqslant \lfloor n!e \rfloor - 1$. Bez zmniejszenia ogólności

---

* $e = \sum_{i=0}^{\infty} \frac{1}{i!}$.

możemy zakładać, że X_1 jest najliczniejszym blokiem naszego podziału. Oznaczając $|X_1| = m_1$ mamy

(5.1) $$m \leqslant m_1 n.$$

Niech X_1 składa się z elementów $x_1^{(1)} < \ldots < x_{m_1}^{(1)}$. Zbiór X_1 jest wolny od sum, zatem żadna z różnic $x_q^{(1)} - x_p^{(1)}$, $1 \leqslant p < q \leqslant m_1$ nie należy do X_1. W szczególności każda spośród $m_1 - 1$ różnic

(5.2) $$x_2^{(1)} - x_1^{(1)}, \ldots, x_{m_1}^{(1)} - x_1^{(1)}$$

należy do $X_2 \cup \ldots \cup X_n$. Znów bez zmniejszenia ogólności możemy zakładać, że do X_2 wpada najwięcej spośród tych różnic, powiedzmy m_2. Mamy oczywiście wtedy $m_2 \geqslant (m_1 - 1)/(n-1)$, czyli

$$m_1 - 1 \leqslant m_2(n-1).$$

Oznaczamy teraz przez $x_1^{(2)} < \ldots < x_{m_2}^{(2)}$ te spośród różnic (5.2), które wpadają do X_2, i kontynuujemy nasz proces. Przypuśćmy, że na pewnym etapie utworzyliśmy już ciągi $x_1^{(i)} < \ldots < x_{m_i}^{(i)}$ dla $i = 1, \ldots, k$ przy czym $m_k > 1$ oraz $x_q^{(i)} - x_p^{(i)} \notin X_1 \cup \ldots \cup X_i$ dla dowolnych i, p, q takich, że $1 \leqslant i \leqslant k$, $1 \leqslant p < q \leqslant m_i$. Bez zmniejszenia ogólności możemy zakładać, że spośród $m_k - 1$ różnic

$$x_2^{(k)} - x_1^{(k)}, \ldots, x_{m_k}^{(k)} - x_1^{(k)}$$

najwięcej – powiedzmy m_{k+1} – wpada do X_{k+1}. Możemy je ponumerować jako $x_1^{(k+1)} < \ldots < x_{m_{k+1}}^{(k+1)}$. Mamy oczywiście

(5.3) $$m_k - 1 \leqslant m_{k+1}(n-k).$$

Co więcej, rozważmy dowolną różnicę $x_q^{(k+1)} - x_p^{(k+1)}$, $1 \leqslant p < q \leqslant m_{k+1}$. Różnica ta nie należy do X_{k+1}, gdyż zbiór ten jest wolny od sum, nie należy też do $X_1 \cup \ldots \cup X_k$ na mocy warunku indukcyjnego, jako że

$$x_q^{(k+1)} - x_p^{(k+1)} = (x_r^{(k)} - x_1^{(k)}) - (x_s^{(k)} - x_1^{(k)}) = x_r^{(k)} - x_s^{(k)},$$

dla pewnych r, s, gdzie $1 \leqslant s < r \leqslant m_k$. Wykazaliśmy więc warunek indukcyjny naszego procesu dla $i = k+1$, i z zasady indukcji wynika, że nierówność (5.3) jest spełniona dla dowolnego k, $1 \leqslant k \leqslant n$ (jeśli $m_k = 0$, to odpowiednich różnic jest nie $m_k - 1$, lecz m_k, i nierówność jest też spełniona).

Udowodnimy teraz przez indukcję względem k, że dla $1 \leqslant k \leqslant n$

(5.4) $$m \leqslant n!\left(\frac{m_k}{(n-k)!} + \frac{1}{(n-k+1)!} + \ldots + \frac{1}{(n-1)!}\right).$$

Dla $k = 1$ nierówność ta redukuje się do wzoru (5.1). Krok indukcyjny wynika z (5.3):

$$n!\left(\frac{m_{k+1}}{(n-k-1)!} + \frac{1}{(n-k)!} - \frac{m_k}{(n-k)!}\right) = n!\,\frac{m_{k+1}(n-k) - (m_k - 1)}{(n-k)!} \geqslant 0,$$

co oznacza, iż prawa strona nierówności (5.4) rośnie ze wzrostem k. Zauważmy, że $m_n \leqslant 1$, gdyż w przeciwnym przypadku otrzymalibyśmy w trakcie naszej konstrukcji liczby $x_1^{(n)} < x_2^{(n)}$, których różnica $x_2^{(n)} - x_1^{(n)}$ nie mogłaby należeć do żadnego ze zbiorów $X_1, \ldots, X_n$. Ostatecznie z (5.4) otrzymujemy, dla $k = n$,

$$m \leqslant n! \sum_{i=0}^{n-1} \frac{1}{i!} = \left(n! \sum_{i=0}^{n} \frac{1}{i!}\right) - 1.$$

Wystarczy teraz wykazać, że

$$n! \sum_{i=0}^{n} \frac{1}{i!} = \lfloor n!e \rfloor. \tag{5.5}$$

Lecz wzór ten wynika stąd, iż lewa strona definiuje liczbę całkowitą mniejszą od $n!e$ o

$$n! \sum_{j=n+1}^{\infty} \frac{1}{j!} = \frac{n!}{(n+1)!}\left(\frac{1}{1} + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots\right) \leqslant$$

$$\leqslant \frac{1}{n+1} \sum_{i=0}^{\infty} \frac{1}{n^i} = \frac{1}{n+1} \cdot \frac{1}{1-1/n} = \frac{n}{n^2-1} < 1 \quad \text{dla } n > 1$$

(dla $n = 1$ wzór (5.5) sprawdzamy bezpośrednio). Dowód twierdzenia jest więc zakończony. □

Oznaczmy przez $S(n)$ najmniejszą spośród liczb m takich, że ilekroć $\{1, \ldots, m\} = X_1 \cup \ldots \cup X_n$, to któryś ze zbiorów X_i nie jest wolny od sum. W tych terminach twierdzenie Schura orzeka, że $S(n)$ istnieje i $S(n) \leqslant \lfloor n!e \rfloor$.

Podamy teraz dolne ograniczenie dla liczb $S(n)$.

LEMAT 5.2 (Schur [1]). *Jeśli $\{1, \ldots, m\} = X_1 \cup \ldots \cup X_n$, gdzie zbiory $X_1, \ldots, X_n$ są wolne od sum, to $\{1, \ldots, 3m+1\}$ można podzielić na $n+1$ zbiorów wolnych od sum.*

Dowód. Niech $X_1 = \{x_1^{(1)}, \ldots, x_{i_1}^{(1)}\}, \ldots, X_n = \{x_1^{(n)}, \ldots, x_{i_n}^{(n)}\}$. Tworzymy zbiory

$$Y_1 = \{3x_1^{(1)}, \ldots, 3x_{i_1}^{(1)}\} \cup \{3x_1^{(1)} - 1, \ldots, 3x_{i_1}^{(1)} - 1\},$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$Y_n = \{3x_1^{(n)}, \ldots, 3x_{i_n}^{(n)}\} \cup \{3x_1^{(n)} - 1, \ldots, 3x_{i_n}^{(n)} - 1\},$$

$$Y_{n+1} = \{1, 4, \ldots, 3m+1\}.$$

Zauważmy, że $Y_1 \cup \ldots \cup Y_n$ zawiera wszystkie liczby naturalne mniejsze od $3m+1$ postaci $3x$ lub $3x+2$ ($0 \leqslant x \leqslant m$), natomiast Y_{n+1} zawiera pozostałe liczby ze zbioru $\{1, \ldots, 3m+1\}$. Wystarczy zatem wykazać, że każdy ze zbiorów Y_j jest wolny od sum. Zbiór Y_{n+1} jest wolny od sum, gdyż suma dwóch liczb postaci $3x+1$ nie jest tej postaci. Niech $a, b \in Y_j$ ($1 \leqslant j \leqslant n$). Jeśli a i b dają różne reszty przy

dzieleniu przez 3, to $a+b = 3(x_{k_1}^{(j)} + x_{k_2}^{(j)}) - 1$ dla pewnych $k_1, k_2 \leqslant i_j$. Gdyby $a+b$ należało do Y_j, to mielibyśmy $a+b = 3x_{k_3} - 1$ dla pewnego $k_3 \leqslant i_j$, a stąd $x_{k_1}^{(j)} + x_{k_2}^{(j)} = x_{k_3}^{(j)}$, wbrew założeniu, że X_j jest wolny od sum. Jeśli $a = 3x_{k_1}^{j}$, $b = 3x_{k_2}^{(j)}$, to $a+b = 3(x_{k_1}^{(j)} + x_{k_2}^{(j)})$ i podobnie $a+b \in Y_j$ pociągałoby za sobą $x_{k_1}^{(j)} + x_{k_2}^{(j)} = x_{k_3}^{(j)}$ dla pewnego $k_3 \leqslant i_j$. Jeśli wreszcie $a = 3x_{k_1}^{(j)} - 1$, $b = 3x_{k_2}^{(j)} - 1$ to $a+b \in Y_{n+1}$, gdyż jest postaci $3x+1$. □

Udowodniony lemat prowadzi do następującego twierdzenia:

Twierdzenie 5.3. $S(n+1) \geqslant 3S(n) - 1$ *i w konsekwencji*

$$S(n) \geqslant \tfrac{1}{2}(3^n + 1).$$

Dowód. Zbiór $\{1, \ldots, S(n)-1\}$ daje się rozłożyć na n zbiorów wolnych od sum. Zatem na mocy lematu 5.2 $S(n+1)$ wynosi co najmniej $3(S(n)-1)+1+1 = 3S(n)-1$. Nierówności $S(n) \geqslant (3^n+1)/2$ dowodzimy przez indukcję. Mamy $S(1) = 2 \geqslant (3^1+1)/2$, oraz jeśli $S(n) \geqslant (3^n+1)/2$, to $S(n+1) \geqslant 3S(n)-1 \geqslant 3(3^n+1)/2 - 1 = (3^{n+1}+1)/2$. □

Twierdzenie 5.3 nie daje najlepszego znanego obecnie dolnego ograniczenia na $S(n)$. Abbott i Hanson [1] wykazali, że $S(n) > c89^{n/4}$ dla pewnej stałej $c > 0$, natomiast Fredricksen [1] poprawił to oszacowanie do $S(n) > c315^{n/5}$ $(3 < 89^{1/4} = 3{,}071 \ldots < 315^{1/5} = 3{,}159 \ldots)$.

Niewiele wiadomo o dokładnych wartościach $S(n)$, nawet dla małych n. Znane są jedynie: $S(1) = 2$, $S(2) = 5$, $S(3) = 14$ oraz $S(4) = 45$ (ta ostatnia wartość została znaleziona przez L. D. Baumerta w 1961 r. za pomocą maszyny cyfrowej). Wiadomo też, że $S(5) \geqslant 158$.

Bezpośrednim wnioskiem z twierdzenia Schura jest fakt, iż zbiór wszystkich liczb naturalnych nie jest sumą skończonej liczby zbiorów wolnych od sum. Zauważmy, że łatwo otrzymać wynikanie w przeciwną stronę stosując twierdzenie 4.3 do rodziny $\mathscr{F} = \{\{x, y, z\}: x, y, z \in \mathbf{N} \wedge x+y = z\}$. Przedstawimy jeszcze inny dowód twierdzenia Schura, pokazujący jednocześnie jego związek z pewnymi liczbami Ramsey'a. Oznaczmy liczbę $R(q_1, \ldots, q_n)$, gdzie $q_1 = \ldots = q_n = k$, przez $R^{(n)}(k)$.

Lemat 5.4. *Dla dowolnego podziału*

$$\{1, \ldots, R^{(n)}(3)-1\} = A_1 \dot{\cup} \ldots \dot{\cup} A_n$$

jeden ze zbiorów A_i nie jest wolny od sum.

Dowód. Utwórzmy graf pełny o $R^{(n)}(3)$ wierzchołkach $0, 1, \ldots, R^{(n)}(3)-1$ i pokolorujmy każdą z krawędzi $\{r, s\}$ kolorem i-tym, gdzie $|r-s| \in A_i$. Zgodnie z definicją liczby $R^{(n)}(3)$ istnieje wtedy trójkąt jednokolorowy, powiedzmy trójkąt koloru i-tego, o wierzchołkach j, k, l. Przyjmując bez zmniejszenia ogólności $j > k > l$ mamy wtedy $j-k$, $k-l$, $j-l \in A_i$, co dowodzi, iż zbiór A_i nie jest wolny od sum, jako że $(j-k)+(k-l) = j-l$. □

Powyższy lemat dowodzi istnienia liczby $S(n)$, oraz oszacowania

(5.6) $$S(n) \leqslant R^{(n)}(3) - 1.$$

Oszacowanie $S(n) \leqslant \lfloor n!e \rfloor$ brakujące do zakończenia drugiego dowodu twierdzenia Schura otrzymamy przez wykazanie analogicznego ograniczenia dla liczb Ramsey'a $R^{(n)}(3)$. Potrzebny nam będzie do tego następujący lemat.

LEMAT 5.5.

$$R^{(n+1)}(3) \leqslant (n+1)\big(R^{(n)}(3) - 1\big) + 2.$$

Dowód. Rozważmy graf pełny o $(n+1)\big(R^{(n)}(3)-1\big)+2$ wierzchołkach, którego krawędzie pokolorowano $n+1$ kolorami. Niech x będzie dowolnym wierzchołkiem tego grafu.

Na mocy zasady podziałowej co najmniej $R^{(n)}(3)$ spośród $(n+1)\big(R^{(n)}(3)-1\big)+1$ krawędzi o końcu w x musi być jednego koloru, powiedzmy czerwonego. Niech te $R^{(n)}(3)$ czerwonych krawędzi łączy x z wierzchołkami $x_1, \ldots, x_s$ ($s = R^{(n)}(3)$). Jeśli któraś z krawędzi $\{x_i, x_j\}$ dla $1 \leqslant i < j \leqslant s$ jest czerwona, to „zamyka" ona czerwony trójkąt. W przeciwnym przypadku mamy pokolorowanie n kolorami krawędzi grafu pełnego o $R^{(n)}(3)$ wierzchołkach $x_1, \ldots, x_s$. Na mocy definicji liczby $R^{(n)}(3)$ graf ten zawiera trójkąt jednokolorowy. □

Możemy teraz przystąpić do pokazania zapowiadanego górnego oszacowania liczb $R^{(n)}(3)$.

TWIERDZENIE 5.6.

$$R^{(n)}(3) \leqslant \lfloor n!e \rfloor + 1.$$

Dowód. Stosujemy indukcję względem n. Dla $n = 1$ mamy $R^{(1)}(3) = 3 = \lfloor e \rfloor + 1$.

Zakładając $R^{(n)}(3) \leqslant \lfloor n!e \rfloor + 1$, z poprzedniego lematu i z (5.5) otrzymujemy

$$\begin{aligned} R^{(n+1)}(3) &\leqslant (n+1)\big(R^{(n)}(3)-1\big)+2 \leqslant (n+1)\lfloor n!e \rfloor + 2 = \\ &= (n+1)n! \sum_{i=0}^{n} \frac{1}{i!} + 2 = (n+1)! \sum_{i=0}^{n+1} \frac{1}{i!} + 1 = \\ &= \lfloor (n+1)!e \rfloor + 1. \ \square \end{aligned}$$

Twierdzenie to w połączeniu z (5.6) daje żądane oszacowanie $S(n) \leqslant \lfloor n!e \rfloor$.

Warto zauważyć, że nierówność w (5.6) nie może być zastąpiona równością. Na przykład $S(3) = 14 < R(3, 3, 3) - 1 = 16$. Oznacza to, że żadne z pokolorowań trzema kolorami krawędzi grafu pełnego o 16 wierzchołkach bez trójkątów jednego koloru nie może być otrzymane z odpowiedniego podziału na zbiory wolne od sum w sposób opisany w dowodzie lematu 5.4.

Pojęcie zbioru wolnego od sum daje się w naturalny sposób wprowadzić w dowolnej grupie $\langle G, + \rangle$. Mówimy, że zbiór $S \subseteq G$ jest *wolny od sum*, jeśli

$(S+S)\cap S=\emptyset$, gdzie $S+S=\{s+t\colon s,\ t\in S\}$. Podobną konstrukcję jak w dowodzie lematu 5.4, można przeprowadzić mając dany podział elementów niezerowych dowolnej grupy na specjalnego rodzaju zbiory wolne od sum. W szczególności, dla $n=3$ można pokazać odpowiedni podział elementów niezerowych pewnej grupy rzędu 16 na trzy zbiory wolne od sum, który generuje pokolorowanie krawędzi grafu pełnego o 16 wierzchołkach bez trójkątów jednego koloru, dowodząc tym samym nierówności $R(3,3,3)\geqslant 17$ (p. zad. 34).

Na zakończenie zauważmy, że nierówność (5.7) w połączeniu z twierdzeniem 5.3 daje następujące oszacowanie na liczby Ramsey'a $R^{(n)}(3)$:

$$R^{(n)}(3)\geqslant \tfrac{1}{2}(3^n+3)$$

(można je nieco poprawić korzystając ze wspomnianych już wzmocnień twierdzenia 5.3).

§ 6. Uogólnienia twierdzenia Schura

Twierdzenie Schura orzeka, iż dla każdego pokolorowania liczb naturalnych skończoną liczbą kolorów równanie $x+y-z=0$ ma rozwiązanie w liczbach x, y, z jednego koloru. O dowolnym równaniu o tej własności będziemy mówili, że jest *regularne*. Oczywiście na mocy twierdzenia 4.3 dane równanie jest regularne wtedy i tylko wtedy, gdy dla każdego naturalnego t istnieje liczba m taka, że dla dowolnego podziału $\{1,\ldots,m\}=A_1\,\dot\cup\,\ldots\,\dot\cup\,A_t$ równanie to ma rozwiązanie w jednym z bloków A_i. Powstaje naturalny problem scharakteryzowania równań regularnych. Dla przypadku równań postaci

$$a_1x_1+\ldots+a_nx_n=0 \tag{6.1}$$

o współczynnikach $a_1,\ldots,a_n$ całkowitych (i niezerowych) prostą odpowiedź dał R. Rado [2].

TWIERDZENIE 6.1. *Równanie* (6.1) *jest regularne wtedy i tylko wtedy, gdy ma nietrywialne rozwiązanie zero-jedynkowe* (*tzn. rozwiązanie w liczbach* 0, 1 *różne od* $x_1=\ldots=x_n=0$).

Dowód. Załóżmy, że równanie (6.1) ma nietrywialne rozwiązanie zero-jedynkowe. Bez zmniejszenia ogólności możemy zakładać, że jest ono postaci

$$a_1\cdot 1+\ldots+a_r\cdot 1+a_{r+1}\cdot 0+\ldots+a_n\cdot 0=0,\qquad r\geqslant 2.$$

Rozważmy równanie

$$ax-ay+bz=0, \tag{6.2}$$

gdzie

$$a=a_1,\qquad b=a_{r+1}+\ldots+a_n.$$

Wystarczy wykazać, że równanie (6.2) jest regularne, gdyż jeśli ma ono rozwiązanie w liczbach x, y, z jednego koloru, to $x_1 = x$, $x_2 = \ldots = x_r = y$, $x_{r+1} = \ldots = x_n = z$ jest rozwiązaniem równania (6.1) w liczbach tego samego koloru:

$$a_1 x + (a_2 + \ldots + a_r)y + (a_{r+1} + \ldots + a_n)z = ax - ay + bz = 0.$$

Udowodnimy teraz, że dla dowolnego $t \geqslant 1$ istnieje liczba m taka, że dla dowolnego podziału $\{1, \ldots, m\} = A_1 \dot\cup \ldots \dot\cup A_t$ równanie (6.2) ma rozwiązanie w jednym z bloków A_i. Stosujemy indukcję względem t. Przypadek $t = 1$ jest oczywisty. Załóżmy, że dla pewnego $t \geqslant 1$ taka liczba m istnieje i rozważmy pokolorowanie zbioru liczb naturalnych $t+1$ kolorami. Na mocy twierdzenia van der Waerdena istnieje wtedy postęp arytmetyczny jednego koloru, powiedzmy czerwonego, długości $bm+1$:

$$s,\ s+d,\ \ldots,\ s+bmd.$$

Jeśli choć jedna z liczb kad, $1 \leqslant k \leqslant m$, jest koloru czerwonego, to daje to rozwiązanie naszego równania w liczbach koloru czerwonego $x = s+b(m-k)d$, $y = s+bmd$, $z = kad$, jako że

$$a(s+b(m-k)d) - a(s+bmd) + bkad = 0.$$

W przeciwnym przypadku mamy do czynienia z pokolorowaniem m liczb ad, $2ad, \ldots, mad$ k kolorami (różnymi od czerwonego). Wobec jednorodności naszego równania, z założenia indukcyjnego wynika istnienie liczb $x, y, z \in \{1, \ldots, m\}$ takich, że xad, yad, zad są jednego koloru i

$$axad - ayad + bzad = 0.$$

Na mocy twierdzenia 4.3 istnieje liczba m^* o tej własności, że dla dowolnego podziału $\{1, \ldots, m^*\} = A_1 \dot\cup \ldots \dot\cup A_{t+1}$ nasze równanie ma rozwiązanie w jednym z bloków A_i (w rzeczywistości powoływanie się na twierdzenie 4.3 nie jest konieczne: wystarczy za m^* przyjąć liczbę $W(t+1, bm+1)$ odpowiednio zwiększoną tak, by $mad \leqslant m^*$). Dowód dostateczności warunku wyrażonego w twierdzeniu jest tym samym zakończony.

Dla dowodu jego konieczności załóżmy, że równanie (6.1) jest regularne, wybierzmy dostatecznie dużą liczbę pierwszą p tak, by

$$p > |a_1| + \ldots + |a_n|, \tag{6.2}$$

i zdefiniujmy pokolorowanie liczb naturalnych na $p-1$ kolorów w następujący sposób: Dla każdej liczby j znajdujemy jednoznaczny rozkład

$$j = p^{\alpha_j}(\beta_j p + \gamma_j), \quad \beta_j \geqslant 0, \quad 1 \leqslant \gamma_j \leqslant p-1$$

i przypisujemy jej kolor γ_j. Wobec regularności naszego równania istnieje dla tego pokolorowania rozwiązanie w liczbach $x_1, \ldots, x_n$ jednakowego koloru. Innymi słowy: istnieją liczby $\gamma, \alpha^{(1)}, \ldots, \alpha^{(n)}, \beta^{(1)}, \ldots, \beta^{(n)}$ takie, że

$$\sum_{i=1}^{n} a_i p^{\alpha^{(i)}}(\beta^{(i)} p + \gamma) = 0.$$

Podzielmy obie strony tej równości przez p^α, gdzie $\alpha = \min\{\alpha^{(i)}\colon 1 \leqslant i \leqslant n\}$, oraz rozważmy powstałą równość modulo p. Otrzymujemy

$$\sum_{i=1}^{n} a_i \varepsilon_i \gamma \equiv 0 \pmod p,$$

gdzie

$$\varepsilon_i = \begin{cases} 0, & \text{jeśli } \alpha^{(i)} > \alpha, \\ 1, & \text{jeśli } \alpha^{(i)} = \alpha, \end{cases}$$

a stąd

$$\sum_{i=1}^{n} a_i \varepsilon_i \equiv 0 \pmod p.$$

Wobec (6.2) powyższa kongruencja jest równoważna równości

$$\sum_{i=1}^{n} a_i \varepsilon_i = 0,$$

co określa nietrywialne rozwiązanie zero-jedynkowe naszego równania, gdyż dla co najmniej jednej wartości i mamy $\alpha^{(i)} = \alpha$, tzn. $\varepsilon_i = 1$. □

Pojęcie regularności równania przenosi się w naturalny sposób na układ dowolnej liczby równań postaci (6.1). Rado podał również charakteryzację układów regularnych tej postaci. Zainteresowanego Czytelnika odsyłamy do oryginalnej pracy Rado [3] (p. też Deuber [1]).

Przechodzimy teraz do innego typu uogólnień twierdzenia Schura. Zaczniemy od następującego prostego faktu.

TWIERDZENIE 6.2. *Jeśli* $|X| \geqslant \lfloor n!e \rfloor$, *to dla dowolnego podziału* $\mathscr{P}(X) = A_1 \dot\cup \ldots \dot\cup A_n$ *istnieje* $i \in \{1, \ldots, n\}$ *oraz niepuste zbiory* $R, S, T \in A_i$ *takie, że* $R \dot\cup S = T$.

Dowód. Bez zmniejszenia ogólności możemy zakładać, że $X = \{1, \ldots, m\}$, $m = \lfloor n!\, e \rfloor$. Rozważmy dowolne pokolorowanie $C\colon \mathscr{P}(X) \to \{1, \ldots, n\}$. Utwórzmy graf pełny o wierzchołkach $1, 2, \ldots, m+1$ i określmy kolor każdej z krawędzi $\{i, j\}$, $i < j$ jako kolor odcinka $\{i, \ldots, j-1\}$ przy pokolorowaniu C. Z twierdzenia 5.6 wnioskujemy, że w naszym grafie istnieje trójkąt o wierzchołkach $i < j < k$ i krawędziach jednego koloru. Określa on zbiory $R = \{i, \ldots, j-1\}$, $S = \{j, \ldots, k-1\}$, $T = \{i, \ldots, k-1\}$, dla których $C(R) = C(S) = C(T)$ oraz $R \dot\cup S = T$. □

Głównym faktem, który w dalszym ciągu udowodnimy, będzie następujące daleko idące uogólnienie twierdzenia 6.2.

TWIERDZENIE 6.3 (Graham i Rothshild [1]). *Dla dowolnych liczb naturalnych* t, k *istnieje* m *takie, że jeśli* $|X| \geqslant m$, *to dla dowolnego pokolorowania* t *kolorami wszystkich podzbiorów zbioru* X *istnieje* k *niepustych i wzajemnie rozłącznych*

zbiorów $S_1, \ldots, S_k \subseteq X$ *takich, że wszystkie* 2^k-1 *sumy postaci* $\bigcup_{j \in J} S_j$, $\emptyset \neq J \subseteq \{1, \ldots, k\}$ *są tego samego koloru.*

Dla dowodu tego twierdzenia (por. Lovász [3]) będziemy potrzebowali następującego lematu.

LEMAT 6.4. *Dla dowolnych liczb naturalnych* t, k *istnieje* m *takie, że jeśli* $|X| \geqslant m$, *to dla dowolnego pokolorowania* t *kolorami wszystkich podzbiorów zbioru* X *istnieje* $2k$ *niepustych i wzajemnie rozłącznych zbiorów* $A_1, \ldots, A_k$, $B_1, \ldots, B_k$ *takich, że dla każdego ustalonego ciągu* $1 \leqslant i_1 < \ldots < i_s \leqslant t$, $1 \leqslant s \leqslant t$ *wszystkie sumy postaci*

$$C_{i_1} \cup \ldots \cup C_{i_s},$$

gdzie C_{i_j} *oznacza dowolny spośród zbiorów* A_{i_j}, B_{i_j}, $A_{i_j} \cup B_{i_j}$, *są tego samego koloru.*

Dowód. Oznaczmy przez $N(t, k)$ najmniejszą z liczb m, o których mowa w tezie lematu (przy założeniu, że taka liczba dla danych t, k istnieje). Do dowodu lematu zastosujemy indukcję względem k. Zauważmy najpierw, że istnienie liczb $N(t, 1)$ wynika z twierdzenia 6.2. Niech więc $k \geqslant 1$ i załóżmy istnienie liczb $N(t, k)$ dla dowolnego t. Wykażemy, że liczby $N(t, k+1)$ istnieją i że dla każdego t mamy $N(t, k+1) \leqslant N(t^{2^a}, 1)+a$, gdzie $a = N(t^2, k)$. Istotnie, niech X będzie zbiorem o liczności $N(t^{2^a}, 1)+a$, zaś T jego podzbiorem o liczności a. Rozważmy dowolne pokolorowanie $C\colon \mathscr{P}(X) \to \{1, \ldots, t\}$. Zdefiniujmy najpierw pewne pokolorowanie

$$C^*\colon \mathscr{P}(X \setminus T) \to \{1, \ldots, t\}^{\mathscr{P}(T)},$$

gdzie kolor $C^*(S)$ dowolnego zbioru $S \subseteq X \setminus T$ jest jednym z t^{2^a} pokolorowań rodziny $\mathscr{P}(T)$, określonym następująco:

$$\big(C^*(S)\big)(Y) = C(S \cup Y) \quad \text{dla każdego } Y \subseteq T.$$

Skoro $|X \setminus T| = N(t^{2^a}, 1)$, to zgodnie z założeniem indukcyjnym istnieją niepuste rozłączne zbiory $A_1, B_1 \subseteq X \setminus T$ takie, że

$$C^*(A_1) = C^*(B_1) = C^*(A_1 \cup B_1),$$

czyli

$$C(A_1 \cup Y) = C(B_1 \cup Y) = C(A_1 \cup B_1 \cup Y) \tag{6.3}$$

dla każdego $Y \subseteq T$. Zdefiniujemy teraz pokolorowanie

$$C^{**}\colon \mathscr{P}(T) \to \{1, \ldots, t\}^2$$

w następujący sposób:

$$C^{**}(Y) = \langle C(Y), C(A_1 \cup Y)\rangle.$$

Pokolorowanie C^{**} używa t^2 kolorów, a $|T| = N(t^2, k)$, tak więc zgodnie z założeniem indukcyjnym istnieją wzajemnie rozłączne niepuste zbiory $A_2, \ldots, A_{k+1}$, $B_2, \ldots, B_{k+1} \subseteq T$ takie, że dla każdego ustalonego ciągu $2 \leqslant i_1 < \ldots < i_s \leqslant t+1$ kolor $C^{**}(C_{i_1} \cup \ldots \cup C_{i_s})$ jest ten sam dla dowolnego wyboru za C_{i_j} zbioru A_{i_j},

B_{i_j} lub $A_{i_j} \cup B_{i_j}$, $j = 1, \ldots, s$. Rozważmy zbiory $A_1, \ldots, A_{k+1}, B_1, \ldots, B_{k+1}$ oraz dowolny ciąg $1 \leqslant i_1 < \ldots < i_s \leqslant t+1$. Jeśli $i_1 > 1$, to $C^{**}(C_{i_1} \cup \ldots \cup C_{i_s})$, a więc tym samym kolor $C(C_{i_1} \cup \ldots \cup C_{i_s})$ jest oczywiście taki sam dla każdego z możliwych zbiorów $C_{i_1} \cup \ldots \cup C_{i_s}$. Jeśli $i_1 = 1$, to kolor $C^{**}(C_{i_2} \cup \ldots \cup C_{i_s})$ jest taki sam dla każdego z możliwych zbiorów $C_{i_2} \cup \ldots \cup C_{i_s}$, a więc zgodnie z definicją pokolorowania C^{**} kolor $C(A_1 \cup C_{i_2} \cup \ldots \cup C_{i_s})$ jest taki sam dla każdego z możliwych zbiorów $Y = C_{i_2} \cup \ldots \cup C_{i_s}$. Korzystając z (6.3) wnioskujemy, że kolor $C(C_{i_1} \cup \ldots \cup C_{i_s})$ jest taki sam dla każdego z możliwych zbiorów $C_{i_1} \cup \ldots \cup C_{i_s}$. □

Możemy teraz przystąpić do zapowiedzianego dowodu twierdzenia 6.3.

D o w ó d t w i e r d z e n i a 6.3. Oznaczmy przez $G(t, k)$ najmniejszą z liczb m, o których mowa w tezie twierdzenia (przy założeniu, że taka liczba dla danych t, k istnieje). Stosujemy indukcję względem k. Oczywiście $G(t, 1) = 1$. Załóżmy teraz istnienie liczby $G(t, k)$ dla pewnego $k \geqslant 1$. Wykażemy, że liczba $G(t, k+1)$ istnieje i spełnia nierówność $G(t, k+1) \leqslant N(t, b)$, gdzie $b = G(t, k)$, natomiast $N(t, b)$ jest liczbą określoną na początku dowodu lematu 6.4. W tym celu rozważmy dowolny zbiór X o liczności $N(t, b)$, oraz dowolne pokolorowanie $C: \mathscr{P}(X) \to \{1, \ldots, t\}$. Zgodnie z poprzednim lematem istnieją niepuste wzajemnie rozłączne zbiory $A_1, \ldots, A_b$, $B_1, \ldots, B_b \subseteq X$ takie, że dla dowolnego ustalonego ciągu $1 \leqslant i_1 < \ldots < i_s \leqslant b$ wszystkie zbiory postaci $C_{i_1} \cup \ldots \cup C_{i_b}$ ($C_{i_j} = A_{i_j}$, B_{i_j} lub $A_{i_j} \cup B_{i_j}$) są tego samego koloru. Zdefiniujmy pokolorowanie

$$C^*: \mathscr{P}(\{1, \ldots, b\}) \to \{1, \ldots, t\}$$

następująco:

$$C^*(\{i_1, \ldots, i_s\}) = C(A_{i_1} \cup \ldots \cup A_{i_s}).$$

Skoro $b = G(t, k)$, to istnieją niepuste wzajemnie rozłączne zbiory $I_1, \ldots, I_k \subseteq \subseteq \{1, \ldots, b\}$ takie, że kolor $C^*\big(\bigcup_{j \in J} I_j\big)$ jest ten sam dla każdego niepustego $J \subseteq \{1, \ldots, k\}$, powiedzmy jest czerwony. Zdefiniujmy teraz następujących $2t$ zbiorów:

$$S_j = \bigcup_{i \in I_j} A_i, \qquad T_j = \bigcup_{i \in I_j} B_i, \qquad j = 1, \ldots, t.$$

Zbiory te są oczywiście niepuste i wzajemnie rozłączne. Wykażemy, że dowolna suma niepustej liczby tych zbiorów ma przy pokolorowaniu C kolor czerwony. Istotnie, niech $\bigcup_{j \in V} S_j \cup \bigcup_{j \in W} T_j$ będzie taką sumą ($V, W \subseteq \{1, \ldots, t\}$, $V \cup W \neq \emptyset$). Oznaczając $I = \bigcup_{j \in V \cap W} I_j$, $I' = \bigcup_{j \in V \setminus W} I_j$, $I'' = \bigcup_{j \in W \setminus V} I_j$ mamy:

$$\begin{aligned} C\Big(\bigcup_{j \in V} S_j \cup \bigcup_{j \in W} T_j\Big) &= C\Big(\bigcup_{j \in V \cap W} (S_j \cup T_j) \cup \bigcup_{j \in V \setminus W} S_j \cup \bigcup_{j \in W \setminus V} T_j\Big) = \\ &= C\Big(\bigcup_{i \in I} (A_i \cup B_i) \cup \bigcup_{i \in I'} A_i \cup \bigcup_{i \in I''} B_i\Big) = \\ &= C\Big(\bigcup_{i \in I \cup I' \cup I''} A_i\Big) = C^*(I \cup I' \cup I'') = C^*\Big(\bigcup_{j \in V \cup W} I_j\Big), \end{aligned}$$

co zgodnie z wyborem zbiorów $I_1, \ldots, I_k$ określa kolor czerwony. Dowód jest zakończony, jako że $2k \geqslant k+1$. □

Inny dowód twierdzenia 6.3 można znaleźć w pracy Nešetřila i Rödla [2]. Łatwym wnioskiem z twierdzenia 6.3 jest następujące uogólnienie twierdzenia Schura.

TWIERDZENIE 6.5 (J. Sanders [1], R. Rado [5], J. Folkman). *Dla dowolnych liczb naturalnych t, k istnieje m takie, że przy dowolnym pokolorowaniu t kolorami zbioru* $\{1, \ldots, m\}$ *istnieje k liczb* $a_1, \ldots, a_k$ *takich, że* $a_1 + \ldots + a_k \leqslant m$ *oraz suma* $\sum_{j \in J} a_j$ *jest tego samego koloru dla każdego niepustego podzbioru* $J \subseteq \{1, \ldots, k\}$.

Dowód. Wybierzmy $m \geqslant G(t, k)$, gdzie $G(t, k)$ określone jest w dowodzie twierdzenia 6.3, i rozważmy dowolne pokolorowanie $C\colon \{1, \ldots, m\} \to \{1, \ldots, t\}$. Zdefiniujmy pokolorowanie $C^*\colon \mathscr{P}(\{1, \ldots, m\}) \setminus \{\emptyset\} \to \{1, \ldots, t\}$ następująco:

$$C^*(Y) = C(|Y|).$$

Na mocy twierdzenia 6.3 istnieją niepuste wzajemnie rozłączne zbiory $S_1, \ldots, S_k$ takie, że kolor

$$C^*\Big(\bigcup_{j \in J} S_j\Big) = C\Big(\Big|\bigcup_{j \in J} S_j\Big|\Big) = C\Big(\sum_{j \in J} |S_i|\Big)$$

jest taki sam dla dowolnego niepustego podzbioru $J \subseteq \{1, \ldots, k\}$. Wystarczy więc przyjąć $a_i = |S_i|$, $i = 1, \ldots, k$. □

Na zakończenie rozważmy sytuację, w której zbiór wszystkich liczb naturalnych kolorujemy skończoną liczbą kolorów. Z twierdzenia 6.5 wynika istnienie dowolnie długich ciągów $a_1, \ldots, a_k$ o własności opisanej w tezie tego twierdzenia. W rzeczywistości istnieje zawsze, jak to pierwszy pokazał Hindman [1], ciąg nieskończony $a_1, a_2, \ldots$ taki, że wszystkie sumy postaci $\sum_{j \in J} a_j$, $\emptyset \neq J \subseteq_{\text{fin}} \boldsymbol{N}$ są tego samego koloru (oczywiście fakt ten nie jest bezpośrednim wnioskiem z twierdzenia 6.5). Prosty dowód tego twierdzenia podał Baumgartner [1].

§ 7. Twierdzenie Halesa–Jewetta

W paragrafie tym udowodnimy twierdzenie podziałowe, które ma ścisły związek z n-wymiarowym uogólnieniem popularnej gry w „kółko i krzyżyk". To interesujące twierdzenie dostarczy nam przy okazji prostego dowodu pewnego wzmocnienia twierdzenia van der Waerdena.

Przypomnijmy, że o rodzinie $\mathscr{F}$ mówimy, że jest t-regularna w X, jeśli dla dowolnego podziału $X = X_1 \dot\cup \ldots \dot\cup X_t$ istnieje $i \in \{1, \ldots, t\}$ oraz zbiór $F \in \mathscr{F}$ taki, że $F \subseteq X_i$. Potrzebny nam będzie następujący prosty lemat.

LEMAT 7.1. *Jeśli rodzina $\mathscr{X}$ jest t-regularna w zbiorze m-elementowym X, a rodzina $\mathscr{Y}$ jest t^m-regularna w zbiorze Y, to rodzina*

$$\mathscr{X} \otimes \mathscr{Y} = \{Z \times T\colon Z \in \mathscr{X} \wedge T \in \mathscr{Y}\}$$

jest t-regularna w zbiorze $X \times Y$.

Dowód. Przyjmijmy, że spełnione są założenia lematu i rozpatrzmy dowolne pokolorowanie $C\colon X \times Y \to \{1, \ldots, t\}$. Zdefiniujmy pokolorowanie $C^*\colon Y \to \{1, \ldots, t\}^X$, które każdemu elementowi $y \in Y$ przyporządkowuje „kolor" będący funkcją $f\colon X \to \{1, \ldots, t\}$ zdefiniowaną następująco:

$$(C^*(y))(x) = C(x, y).$$

Pokolorowanie C^* używa t^m kolorów, a więc zgodnie z naszymi założeniami istnieje jednokolorowy zbiór $T \in \mathscr{Y}$, tzn. dla każdego ustalonego $x \in X$ kolor $C(x, y)$ jest stały dla $y \in T$. Możemy więc zdefiniować pokolorowanie $C^{**}\colon X \to \{1, \ldots, t\}$ następująco:

$$C^{**}(x) = C(x, y) \quad \text{dla } y \in T.$$

Na mocy t-regularności $\mathscr{X}$ w X istnieje zbiór Z taki, że kolor $C^{**}(x)$ jest stały dla $x \in Z$. W konsekwencji kolor $C(x, y)$ jest stały dla $\langle x, y\rangle \in Z \times T$.□

Niech $k > 0$, $I_k = \{1, \ldots, k\}$. Zbiór

$$I_k^n = \{\langle x_1, \ldots, x_n\rangle\colon 1 \leqslant x_1 \leqslant k \wedge \ldots \wedge 1 \leqslant x_n \leqslant k\}$$

będziemy nazywali *kostką n-wymiarową na zbiorze* $\{1, \ldots, k\}$. Załóżmy, że dana jest dowolna funkcja $f\colon I_k \to I_k^n$ o następującej własności:

Jeśli oznaczymy $f(x) = \langle f_1(x), \ldots, f_n(x)\rangle$, to każda z funkcji f_i albo jest stała (tzn. $f_i(x) = x_0$ dla pewnego $x_0 \in I_k$ i wszystkich $x \in I_k$), albo jest identycznością (tzn. $f_i(x) = x$ dla wszystkich $x \in I_k$), przy czym nie wszystkie funkcje f_i są stałe.

Zbiór $L = f(I_k)$ nazywamy wtedy *prostą* w L_k^n, funkcję zaś f *parametryzacją* tej prostej.

Łatwo zauważyć, że każda prosta ma dokładnie jedną parametryzację.

TWIERDZENIE 7.2 (Hales i Jewett [1]). *Dla dowolnych liczb naturalnych t, k istnieje liczba n o następującej własności:*

Dla dowolnego $m \geqslant n$, jeśli $I_k^m = A_1 \cup \ldots \cup A_t$, to dla pewnego $i \in \{1, \ldots, t\}$ zbiór A_i zawiera prostą.

Dowód. Oznaczmy przez $H(t, k)$ najmniejszą z liczb n, o których mowa w tezie twierdzenia (przy założeniu, że dla danych t, k taka liczba istnieje). Dla dowodu twierdzenia zastosujemy indukcję na zbiorze par $\langle k, t\rangle$ $(k, t > 0)$ uporządkowanych leksykograficznie.

Istnienie liczb $H(1, k)$, $H(t, 1)$ jest oczywiste dla dowolnych $t, k > 0$. Niech zatem $t, k > 1$ i niech — na mocy założenia indukcyjnego — istnieją liczby

$H(t-1, k)$ oraz $H(j, k-1)$ dla dowolnego $j > 0$. Przyjmijmy $r = H(t-1, k)+1$ i określmy liczby $n_1, n_2, \ldots, n_r$ indukcyjnie, w następujący sposób:

$$n_1 = H(t, k-1), \qquad p_1 = |I_{k-1}^{n_1}| = (k-1)^{n_1},$$
$$n_2 = H(t^{p_1}, k-1), \qquad p_2 = p_1 |I_{k-1}^{n_2}| = p_1 (k-1)^{n_2},$$
$$\ldots\ldots\ldots\ldots \qquad \ldots\ldots\ldots\ldots\ldots\ldots$$
$$n_{r-1} = H(t^{p_{r-2}}, k-1), \qquad p_{r-1} = p_{r-2} |I_{k-1}^{n_{r-1}}| = p_{r-2}(k-1)^{n_{r-1}},$$
$$n_r = H(t^{p_{r-1}}, k-1).$$

Niech $q = n_1 + \ldots + n_r$. Wykażemy, że $H(t, k) \leqslant q$. Niech zatem $I_k^q = A_1 \cup \ldots \cup A_t$. Mamy wtedy $I_{k-1}^q = B_1 \cup \ldots \cup B_t$, gdzie $B_i = A_i \cap I_{k-1}^q$ dla $1 \leqslant i \leqslant t$. Skoro $p_i = |I_{k-1}^{n_1} \times \ldots \times I_{k-1}^{n_i}|$, to przez $(r-1)$-krotne zastosowanie lematu 7.1 otrzymujemy następujący wniosek: Istnieje wskaźnik i_0, $1 \leqslant i_0 \leqslant t$, oraz proste $L_1 \subseteq I_{k-1}^{n_i}, \ldots, L_r \subseteq I_{k-1}^{n_r}$ takie, że

$$L_1 \times \ldots \times L_r \subseteq B_{i_0}.$$

Istotnie, jeśli założymy, że dla pewnego $i < r$ rodzina zbiorów postaci $L_1 \times \ldots \times L_i$ (gdzie L_j jest prostą w $I_{k-1}^{n_j}$, $1 \leqslant j \leqslant i$) jest t-regularna w $I_{k-1}^{n_1+\ldots+n_i}$, to wobec definicji liczby $n_{i+1} = H(t^{p_i}, k-1)$ i lematu 7.1 rodzina zbiorów postaci $(L_1 \times \ldots \times L_i) \times L_{i+1}$ jest t-regularna w $I_{k-1}^{n_1+\ldots+n_i+n_{i+1}}$. Prostym $L_1, \ldots, L_r$ odpowiadają pewne parametryzacje $f^{(1)}, \ldots, f^{(r)}$. Rozważmy funkcję

$$g\colon I_k^{r-1} \to Z = f^{(1)}(I_k) \times \ldots \times f^{(r-1)}(I_k) \times \{f^{(r)}(k)\} \subseteq I_k^q$$

(parametryzacje $f^{(i)}$ traktujemy tu jako rozszerzone w naturalny sposób z I_{k-1} na I_k) określoną następująco:

$$g(x_1, \ldots, x_{r-1}) = f^{(1)}(x_1)^\frown \ldots {}^\frown f^{(r-1)}(x_{r-1})^\frown f^{(r)}(k)$$

($\langle a_1, \ldots, a_p\rangle^\frown \langle b_1, \ldots, b_s\rangle$ oznacza $\langle a_1, \ldots, a_p, b_1, \ldots, b_s\rangle$). Niech teraz $I_k^{r-1} = C_1 \cup \ldots \cup C_t$, gdzie $C_i = g^{-1}(A_i)$ dla $1 \leqslant i \leqslant t$. Jeśli $C_{i_0} = \emptyset$, to wobec równości $r-1 = H(t-1, k)$ mamy $L \subseteq C_i$ dla pewnego i oraz prostej $L \subseteq I_k^{r-1}$. Lecz zauważmy, że funkcja g przeprowadza proste w I_k^{r-1} na proste w I_k^q. Zatem zbiór A_i zawiera prostą $g(L)$.

Niech więc $C_{i_0} \neq \emptyset$. Istnieją wtedy $x_1, \ldots, x_{r-1} \in I_k$ takie, że

$$y = \langle y_1, \ldots, y_q\rangle = f^{(1)}(x_1)^\frown \ldots {}^\frown f^{(r-1)}(x_{r-1})^\frown f^{(r)}(k) \in A_{i_0} \cap Z.$$

Rozważmy funkcję $h\colon I_k \to I_k^q$ określoną następująco:

$$h(x) = \langle h_1(x), \ldots, h_q(x)\rangle,$$

$$h_i(x) = \begin{cases} y_i, & \text{jeśli } y_i \in I_{k-1}, \\ x, & \text{jeśli } y_i = k. \end{cases}$$

Funkcja h jest parametryzacją pewnej prostej $L \subseteq I_k^q$ (zauważmy, że y zawiera $f^{(r)}(k)$ jako końcowy odcinek współrzędnych, zatem $y_i = k$ dla pewnego i, co

oznacza, iż nie wszystkie funkcje h_i są stałe). Wykażemy, że $L \subseteq A_{i_0}$. Istotnie, mamy $h(I_{k-1}) \subseteq L_1 \times \ldots \times L_r \subseteq B_{i_0} \subseteq A_{i_0}$, $h(k) = y \in A_{i_0}$, a stąd $h(I_k) = h(I_{k-1}) \cup \cup \{h(k)\} \subseteq A_{i_0}$. □

Jeśli w definicji prostej w I_k^n dopuścimy takie parametryzacje $f(x) = \langle f_1(x), \ldots, f_n(x) \rangle$, dla których pewne funkcje f_i mogą być postaci $f(x) = k+1-x$ dla $x \in I_k$, to otrzymamy pewną szerszą klasę podzbiorów kostki I_k^n. Podzbiory te będziemy nazywali *liniami*. Twierdzenie Halesa–Jewetta pozostaje oczywiście prawdziwe, jeśli proste zastąpimy liniami, przy czym odpowiednie liczby $H^*(t, k)$ są wtedy nie większe niż $H(t, k)$.

Wiadomo, że gra w „kółko i krzyżyk" może zakończyć się remisem (brak linii złożonej z kółek oraz brak linii złożonej z krzyżyków, przy wypełnionych wszystkich 9 klatkach). Fakt ten oznacza nic innego jak $H^*(2, 3) > 2$. W tym kontekście twierdzenie Halesa–Jewetta orzeka, iż przy dostatecznie dużym n (a mianowicie $n \geqslant H^*(t, 3)$) n-wymiarowa gra w „kółko i krzyżyk", w której uczestniczy t graczy, musi zakończyć się zwycięstwem któregoś z graczy.

Wiele twierdzeń podziałowych może być podstawą do opracowania gier, w których niemożliwy jest remis. Rozważmy jedną z takich możliwości: Dla danego grafu G obieramy $r(G, G)$ wierzchołków (por. § 3). Każdy z graczy może połączyć dowolne dwa nie połączone jeszcze wierzchołki, pierwszy gracz czerwoną krawędzią, a drugi niebieską. Gracze dodają kolejno po jednej krawędzi. Wygrywa ten, kto jako pierwszy utworzy graf „swojego" koloru izomorficzny z G. Z definicji liczby $r(G, G)$ wynika, że remis w takiej grze jest niemożliwy.

Twierdzenie van der Waerdena jest prostym wnioskiem z twierdzenia Halesa–Jewetta. Istotnie, jeśli każdemu punktowi $\langle x_1, \ldots, x_n \rangle \in I_k^n$ przyporządkujemy liczbę $h(x_1, \ldots, x_n) = x_1 + \ldots + x_n$, to dowolnemu podziałowi $h(I_k^n) = A_1 \dot{\cup} \ldots \dot{\cup} A_t$ odpowiada podział

$$I_k^n = B_1 \dot{\cup} \ldots \dot{\cup} B_t, \qquad \text{gdzie } B_i = \{x \in I_k^n \colon h(x) \in A_i\}.$$

Jeśli $n \geqslant H(t, k)$, to któryś ze zbiorów B_i zawiera pewną prostą L. Lecz wtedy A_i zawiera postęp arytmetyczny o długości k. Wynika to stąd, że jeśli prosta L ma parametryzację $f(x) = \langle f_1(x), \ldots, f_n(x) \rangle$, gdzie funkcje $f_{i_1}, \ldots, f_{i_r}$ są stałe a funkcje $f_{j_1}, \ldots, f_{j_q}$ są identycznościami, to $h(L) = \{a + qi \colon i \in I_k\}$, gdzie $a = f_{i_1}(1) + \ldots + f_{i_r}(1)$.

Stosując twierdzenie Halesa–Jewetta możemy wzmocnić twierdzenie van der Waerdena w następujący sposób:

TWIERDZENIE 7.3 (Spencer [1]). *Dla dowolnych t, $k > 1$ istnieje skończony zbiór liczb naturalnych A spełniający następujące dwa warunki:*

(a) *A nie zawiera postępu arytmetycznego długości $k+1$,*

(b) *Dla każdego podziału $A = A_1 \cup \ldots \cup A_t$ istnieje $i \in \{1, \ldots, t\}$ takie, że zbiór A_i zawiera postęp arytmetyczny długości k.*

Dowód. Oczywiście twierdzenie Halesa–Jewetta jest prawdziwe (bez zmiany liczb $H(t, k)$), jeśli rozpatrujemy kostki na zbiorze $\bar{I}_k = \{0, \ldots, k-1\}$ zamiast

$I_k = \{1, \ldots, k\}$. Niech $n \geqslant H(t, k)$, i niech $p > k$ będzie liczbą pierwszą. Rozpatrzmy funkcję $h: \bar{I}_k^n \to N_0$ zdefiniowaną następująco:

$$h(x_0, \ldots, x_{n-1}) = x_0 + x_1 p + \ldots + x_{n-1} p^{n-1}$$

(zauważmy, że również współrzędne numerujemy od 0 do $n-1$, a nie od 1 do n). Wykażemy, że zbiór $A = h(\bar{I}_k^n)$ spełnia warunki (a) i (b). Warunek (b) wykazujemy analogicznie jak poprzednio przy dowodzie twierdzenia van der Waerdena. Różnica polega jedynie na tym, że obecnie, jeśli pewna prosta $L \subseteq \bar{I}_k^n$ ma parametryzację $f(x) = \langle f_0(x), \ldots, f_{n-1}(x) \rangle$, gdzie funkcje $f_{i_1}, \ldots, f_{i_r}$ są stałe a funkcje $f_{j_1}, \ldots, f_{j_q}$ identycznościami, to $h(L) = \{a + di: i \in \bar{I}_k\}$ gdzie

$$a = f_{i_1}(1)p^{i_1} + \ldots + f_{i_r}(1)p^{i_r},$$
$$d = p^{j_1} + \ldots + p^{j_q}.$$

Wykażemy teraz warunek (d). Załóżmy, że zbiór A zawiera postęp a, $a + d, \ldots, a + kd$, gdzie $d \neq 0$. Liczba d ma pewne rozwinięcie $d = d_i p^i + d_{i+1} p^{i+1} + \ldots + d_{n-1} p^{n-1}$ przy podstawie p, gdzie $d_i \neq 0$. Podobnie $a = \sum_{j=1}^{n} a_j p^j$. Ponieważ d_i jest pierwszym niezerowym współczynnikiem w rozwinięciu d, zatem i-ty współczynnik w rozwinięciu $a + sd$ przy podstawie p jest równy $a_i + sd_i \pmod p$ dla $0 \leqslant s \leqslant k$. Liczby $a_i + sd_i \pmod p$, $0 \leqslant s \leqslant k$, należą do zbioru $\{0, \ldots, k-1\}$, gdyż liczby $a + sd$ należą do zbioru A (a każda liczba ma dokładnie jedno rozwinięcie przy podstawie p). Lecz z drugiej strony liczby $a_i + sd_i \pmod p$, $0 \leqslant s \leqslant k$, są parami różne, gdyż p jest liczbą pierwszą, $k < p$ i $d_i < p$ (gdyby dla dwu różnych $s_1, s_2 \in \{0, \ldots, k\}$ $a_i + s_1 d_i \equiv a_i + s_2 d_i \pmod p$ to mielibyśmy $(s_1 - s_2)d_i \equiv 0 \pmod p$). Otrzymana sprzeczność dowodzi, iż zbiór A nie może zawierać postępu arytmetycznego o długości $k+1$, co kończy dowód twierdzenia (ściśle rzecz biorąc, należałoby zbiór A zamienić na zbiór $\{a+1: a \in A\}$, jako że zera nie uważamy za liczbę naturalną). □

§ 8. Inne twierdzenia podziałowe

Klasyczne twierdzenie Ramsey'a możemy wyrazić w terminach zbiorów częściowo uporządkowanych w następujący sposób: Dla dowolnych r, t, $k \in \mathbf{N}$ istnieje liczba n o tej własności, że ilekroć $|X| \geqslant n$ i wszystkie elementy rangi r w zbiorze częściowo uporządkowanym $\langle \mathscr{P}(X), \subseteq \rangle$ pokolorujemy t kolorami, to istnieje taki element $Y \in \mathscr{P}(X)$ rangi k, że wszystkie elementy $Z \subseteq Y$ rangi r są tego samego koloru.

Niech $\mathbf{P}_1, \mathbf{P}_2, \ldots$ będzie dowolnym ciągiem zbiorów częściowo uporządkowanych (relację porządku będziemy oznaczali w każdym z nich przez $\leqslant$). Przez analogię do powyższego sformułowania twierdzenia Ramsey'a będziemy mówili, że ciąg $\mathbf{P}_1, \mathbf{P}_2, \ldots$ ma *własność Ramsey'a*, jeśli dla dowolnych r, t, $k \geqslant 0$ istnieje n

takie, że ilekroć $m \geq n$ i wszystkie elementy rangi r w P_m pokolorujemy t kolorami, to istnieje w P_m element y rangi k taki, że wszystkie elementy $z \leq y$ rangi r są tego samego koloru. Tak więc twierdzenie Ramsey'a wyraża fakt, że ciąg $\mathscr{P}_1, \mathscr{P}_2, \ldots$ ma własność Ramsey'a, gdzie $\mathscr{P}_i$ jest zbiorem $\mathscr{P}(\{1, \ldots, i\})$ uporządkowanym przez inkluzję (lub, co na jedno wychodzi, dowolną skończoną algebrą Boole'a o i atomach).

Okazuje się, że własność Ramsey'a przysługuje wielu ważnym ciągom zbiorów częściowo uporządkowanych. Oto niektóre z nich:

(a) $\Pi_1, \Pi_2, \ldots$, gdzie Π_i jest zbiorem wszystkich podziałów zbioru $\{1, \ldots, i\}$ uporządkowanych przez relację rozdrobnienia ($\pi \leq \delta$, jeśli każdy blok podziału δ jest sumą pewnej liczby bloków podziału π).

(b) $\Pi_1^*, \Pi_2^*, \ldots$, gdzie Π_i^* jest zbiorem częściowo uporządkowanym dualnym względem Π_i.

(c) $\mathscr{L}(1, q), \mathscr{L}(2, q), \ldots$, gdzie $\mathscr{L}(i, q)$ jest kratą podprzestrzeni przestrzeni liniowej wymiaru i nad ciałem $GF(q)$ (por. rozdz. 1, § 12).

(d) $\mathscr{A}(1, q), \mathscr{A}(2, q), \ldots$, gdzie $\mathscr{A}(i, q)$ jest kratą podprzestrzeni przestrzeni afinicznej wymiaru i nad ciałem $GF(q)$ (por. rozdz. 1, § 12).

Dla ciągu (a) własność Ramsey'a jest prostym wnioskiem z faktu, że odcinek $[0, \pi] \subseteq \Pi_{2n}$, gdzie $0 = \{\{1\}, \ldots, \{2n\}\}$, $\pi = \{\{1, 2\}, \{3, 4\}, \ldots, \{2n-1, 2n\}\}$ jest izomorficzny z $\mathscr{P}_n$. Dowód własności Ramsey'a dla ciągu (b) jest trudniejszy. Został on podany przez Grahama i Rothschilda jako wniosek z tzw. twierdzenia Ramsey'a dla zbiorów n-parametrowych [1], które zresztą pozwoliło również na udowodnienie własności Ramsey'a dla ciągów (c) i (d) w szczególnym przypadku $r \leq 1$.

Dowód dla dowolnego r, jak również pewne bardzo ogólne twierdzenie podziałowe sformułowane w języku teorii kategorii podali Leeb, Graham i Rothschild [1].

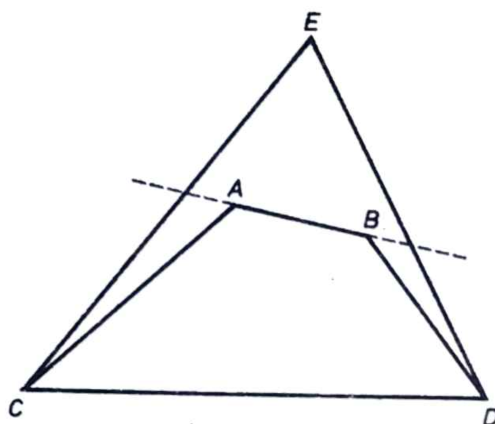
§ 9. Geometryczne zastosowanie twierdzenia Ramsey'a

Podamy obecnie pewne zastosowanie twierdzenia Ramsey'a pochodzące od Erdösa i Szekeresa [1]. Możemy je sformułować nieformalnie w następujący sposób: Z dowolnego rozmieszczenia na płaszczyźnie „dużej" liczby punktów, z których żadne trzy nie leżą na jednej prostej, można wybrać „spory" podzbiór punktów, będących zbiorem wierzchołków pewnego wielokąta wypukłego. Będziemy potrzebowali następujących dwóch prostych lematów geometrycznych.

LEMAT 9.1. *Spośród dowolnych pięciu punktów płaszczyzny, z których żadne trzy nie leżą na jednej prostej, cztery są wierzchołkami czworokąta wypukłego.*

Dowód. Jeśli otoczka wypukła naszych pięciu punktów (tzn. najmniejszy zawierający je podzbiór wypukły płaszczyzny) jest czworokątem lub pięciokątem, to teza lematu jest oczywista. Jeśli jest trójkątem, to dwa punkty — powiedzmy A

i B — leżą wewnątrz tego trójkąta. Pewne dwa wierzchołki naszego trójkąta — oznaczmy je przez C i D — leżą po jednej stronie prostej przechodzącej przez A i B. Łatwo zauważyć, że A, B, C, D są wierzchołkami czworokąta wypukłego (p. rys. 24). □



Rys. 24. Do dowodu lematu 9.1

LEMAT 9.2. *Niech będzie danych n punktów płaszczyzny, z których żadne trzy nie leżą na jednej prostej. Jeśla każde cztery z nich są wierzchołkami czworokąta wypukłego, to punkty te są wierzchołkami n-kąta wypukłego.*

Dowód. Załóżmy, że otoczka wypukła zbioru naszych n punktów jest m-kątem wypukłym, gdzie $m < n$. Niech jego wierzchołkami będą $A_1, \ldots, A_m$. Co najmniej jeden z n punktów leży wewnątrz tego m-kąta, musi więc leżeć wewnątrz któregoś z trójkątów $A_1A_2A_3$, $A_1A_3A_4, \ldots, A_1A_{m-1}A_m$ (nie może leżeć na krawędzi żadnego z tych trójkątów, gdyż mielibyśmy wtedy trzy punkty na jednej prostej). Lecz punkt ten wraz z wierzchołkami trójkąta, który go zawiera, określa cztery punkty nie będące wierzchołkami czworokąta wypukłego. Otrzymana w ten sposób sprzeczność z założeniami lematu dowodzi, że musi być $m = n$. □

Zauważmy, że w dowodach obu lematów korzystaliśmy z następującego prostego faktu: Otoczka wypukła dowolnego skończonego zbioru S punktów płaszczyzny jest wielokątem wypukłym, którego każdy z wierzchołków należy do S (p. zad. 39).

A oto zapowiedziane zastosowanie twierdzenia Ramsey'a:

TWIERDZENIE 9.3 (Erdös i Szekeres [1]). *Jeśli $n \geqslant R_4(m, 5)$, to dowolny zbiór n punktów płaszczyzny, z których żadne trzy nie leżą na jednej prostej, zawiera m punktów stanowiących wierzchołki n-kąta wypukłego.*

Dowód. Niech X będzie zbiorem n punktów płaszczyzny, z których żadne trzy nie leżą na jednej prostej. Rozważmy podział $\mathscr{P}_4(X) = A_1 \dot\cup A_2$, gdzie do A_1 należą zbiory wierzchołków czworokątów wypukłych, do A_2 natomiast zbiory wierzchołków czworokątów wklęsłych. Z definicji liczby $R_4(m, 5)$ wynika, że albo istnieje podzbiór $Y \subseteq X$, $|Y| = m$, taki, że każde cztery różne punkty z Y stanowią

wierzchołki czworokąta wypukłego, albo też istnieje w X pięć punktów, z których każde cztery są wierzchołkami czworokąta wklęsłego. Na mocy lematu 9.1 ten ostatni przypadek jest niemożliwy, zachodzi więc pierwsza z możliwości. Lecz lemat 9.2 orzeka, iż Y jest wtedy zbiorem wierzchołków m-kąta wypukłego. □

Oznaczmy przez N_m najmniejszą z liczb n, dla których spełniona jest teza twierdzenia 9.3. Twierdzenie mówi, że $N_m \leqslant R_4(m, 5)$. Można wykazać, że $N_3 = 3 = 2+1$, $N_4 = 5 = 2^2+1$, $N_5 = 9 = 2^3+1$, co prowadzi do przypuszczenia, dotychczas nierozstrzygniętego, iż $N_m = 2^{m-2}+1$ dla dowolnego $m \geqslant 3$.

§ 10. Własności podziałowe zbiorów nieskończonych

Wiele z przedstawionych w tym rozdziale twierdzeń podziałowych ma ciekawe uogólnienia na zbiory nieskończone. Zaczniemy od najbardziej elementarnych.

Uogólniona zasada szufladkowa Dirichleta. Jeśli $X = \bigcup_{i\in I} X_i$, gdzie $|X| > |I|$, to istnieje $i \in I$ takie, że $|X_i| \geqslant 2$.

Dokładniejsze szacowanie liczności zbiorów X_i jest przedmiotem arytmetyki liczb kardynalnych i rozważań na temat liczb kardynalnych regularnych i osobliwych. Zainteresowanego czytelnika odsyłamy do odpowiedniej literatury (p. np. Kuratowski i Mostowski [1]), tu odnotujemy natomiast jedynie oczywiste wzmocnienie zasady szufladkowej w szczególnym przypadku, gdy zbiór X jest nieskończony a zbiór I skończony:

Uogólniona zasada podziałowa. Jeśli X jest zbiorem nieskończonym i $X = X_1 \cup \ldots \cup X_t$, to istnieje $i \in \{1, \ldots, t\}$ takie, że zbiór X_i jest nieskończony.

Udowodnimy teraz nieskończoną wersję twierdzenia Ramsey'a. Zauważmy, że ze skończonego twierdzenia Ramsey'a w oczywisty sposób wynika fakt, iż jeśli zbiór X jest nieskończony i zbiór $\mathscr{P}_r(X)$ pokolorujemy skończoną liczbą kolorów, to istnieją zbiory $Y \subseteq X$ dowolnie dużej, lecz skończonej liczności takie, że zbiór $\mathscr{P}_r(Y)$ jest pokolorowany jednym kolorem. Wykażemy teraz, że istnieje również zawsze nieskończony zbiór Y o tej własności. Dowód będzie przebiegał zupełnie analogicznie jak drugi dowód skończonego twierdzenia Ramsey'a przedstawiony w § 1. Potrzebny nam będzie najpierw pewien nieskończony odpowiednik lematu 1.2, zwany zwykle *lematem Königa*. Przypomnijmy, że przez rząd elementu w drzewie $\langle X, \leqslant \rangle$ rozumiemy liczbę jego bezpośrednich następników. Będziemy mówili, że rząd drzewa jest *niemal skończony*, jeśli rząd każdego elementu tego drzewa jest skończony. Każdy maksymalny łańcuch w drzewie będziemy nazywali *gałęzią*. Łatwo zauważyć, że korzeń drzewa jest elementem każdej gałęzi, oraz że każdy łańcuch można rozszerzyć do gałęzi (jest to bezpośredni wniosek z lematu Kuratowskiego–Zorna).

LEMAT 10.1 (lemat Königa [1]). *Jeśli $T = \langle X, \leqslant \rangle$ jest drzewem nieskończonym rzędu niemal skończonego, to T zawiera gałąź nieskończoną.*

Dowód. Dla każdego $x \in X$ oznaczmy $T_x = \{y \in X\colon x \leqslant y\}$. Zauważmy, że jeśli zbiór T_x jest nieskończony i $y_1, \ldots, y_t$ są wszystkimi bezpośrednimi następnikami elementu x, to co najmniej jeden ze zbiorów $T_{y_1}, \ldots, T_{y_t}$ jest nieskończony. Wynika to bezpośrednio z uogólnionej zasady podziałowej i z faktu, iż $T_x = \{x\} \cup T_{y_1} \cup \ldots \cup T_{y_t}$. Możemy więc zdefiniować indukcyjnie ciąg $x_1, x_2, \ldots$, gdzie x_1 jest korzeniem drzewa, natomiast x_{i+1} jest bezpośrednim następnikiem elementu x_i takim, że zbiór $T_{x_{i+1}}$ jest nieskończony. Zbiór $L = \{x_i\colon i \in N\}$ jest oczywiście łańcuchem nieskończonym. Łatwo też zauważyć, że L jest gałęzią. Istotnie, przypuśćmy, że w T istnieje łańcuch $L \cup \{z\}$, $z \notin L$. Każdy element drzewa ma, z definicji, skończoną rangę, łańcuch L natomiast zawiera elementy dowolnej rangi. Stąd $r(z) = r(x_i)$ dla pewnego i, i w konsekwencji nie może być ani $z < x_i$, ani $x_i < z$, co przeczy naszemu przypuszczeniu, iż $L \cup \{z\}$ jest łańcuchem. □

Możemy teraz przystąpić do dowodu zapowiedzianej już nieskończonej wersji twierdzenia Ramsey'a.

TWIERDZENIE 10.2 (Ramsey [1]). *Niech X będzie zbiorem nieskończonym i niech $\mathscr{P}_r(X) = A_1 \cup \ldots \cup A_t$. Wówczas istnieje $i \in \{1, \ldots, t\}$ oraz zbiór nieskończony $Y \subseteq X$ taki, że $\mathscr{P}_r(Y) \subseteq A_i$.*

Dowód. Ograniczymy się do przypadku $r = 2$, $t = 2$, pozostawiając łatwe uogólnienie Czytelnikowi. Podobnie jak w drugim dowodzie skończonego twierdzenia Ramsey'a konstruujemy drzewo $T = \langle D, \leqslant \rangle$, którego elementami są pewne ciągi skończone postaci $i_1, \ldots, i_p$, gdzie $p \geqslant 0$ oraz $i_m \in \{1, 2\}$ dla $1 \leqslant m \leqslant p$. Porządek $\leqslant$ określony jest też tak jak w przypadku skończonym: $w_1 \leqslant w_2$, jeśli ciąg w_1 jest odcinkiem początkowym ciągu w_2. Każdemu elementowi $w \in D$ przyporządkowany będzie pewien zbiór $S_w \subseteq X$ oraz element $x_w \in S_w$. Jako korzeń drzewa przyjmujemy ciąg pusty ε, oraz przyjmujemy $S_\varepsilon = X$, za x_ε zaś przyjmujemy dowolny element zbioru X. Konstrukcja zbiorów S_w i elementów x_w jest indukcyjna względem długości ciągu w. Mając dany element $w = i_1 \ldots i_p$ drzewa oraz odpowiadający mu zbiór S_w i element x_w definiujemy zbiory

$$S_{wj} = \{y \in S_w\colon \{x_w, y\} \in A_j\}, \qquad j = 1, 2,$$

oraz dla tych spośród zbiorów S_{wj}, które są niepuste, dołączamy do zbioru elementów naszego drzewa odpowiadające im ciągi wj, oraz wybieramy dowolne elementy $x_{wj} \in S_{wj}$. Wykażemy, że drzewo $T = \langle D, \leqslant \rangle$ otrzymane w wyniku tej konstrukcji jest nieskończone, co więcej, że istnieje nieskończenie wiele elementów w D, dla których zbiór S_w jest nieskończony. Istotnie, gdyby liczba tych elementów była skończona, to istniałby wśród nich (co najmniej jeden) element w_0 o największej randze. Z naszej konstrukcji wynika, że $S_{w_0} = \{x_{w_0}\} \cup S_{w_0 1} \cup S_{w_0 2}$, a więc na mocy uogólnionej zasady podziałowej co najmniej jeden spośród zbiorów $S_{w_0 j}$, $j = 1, 2$, byłby nieskończony. Lecz wtedy odpowiadający mu element $w_0 j$ byłby elementem drzewa i $r(w_0 j) = r(w_0) + 1$, wbrew naszemu wyborowi elementu w_0.

Skoro nasze drzewo jest nieskończone, z lematu Königa wnioskujemy o istnieniu nieskończonej gałęzi $w_1 < w_2 < \ldots$ Rozpatrzmy odpowiadający jej ciąg $y_1, y_2, \ldots$, gdzie $y_i = x_{w_i}$. Z naszej konstrukcji wynika, że każdy element y_i jest albo pierwszego rodzaju, tzn. $\{y_i, y_j\} \in A_1$ dla każdego $j > i$, albo (w przeciwnym przypadku) drugiego rodzaju, tzn. $\{y_i, y_j\} \in A_2$ dla każdego $j > i$. Oznaczając przez U_i zbiór elementów i-tego rodzaju mamy $\{y_i\colon i \in N\} = U_1 \dot\cup U_2$. Korzystając znów z uogólnionej zasady podziałowej wnioskujemy, że jeden ze zbiorów U_1, U_2 — bez zmniejszenia ogólności możemy założyć, że U_1 — jest nieskończony. Wykażemy, że $\mathscr{P}_2(U_1) \subseteq A_1$. Istotnie, jeśli $\{y_i, y_j\} \in \mathscr{P}_2(U_1)$, gdzie $i<j$, to $\{y_i, y_j\} \in A_1$, gdyż y_i jest pierwszego rodzaju. □

Zauważmy, że jeśli zbiór X jest przeliczalny, to nieskończone twierdzenie Ramsey'a orzeka, iż przy dowolnym pokolorowaniu dwoma kolorami krawędzi grafu pełnego G o zbiorze wierzchołków X powstaje podgraf o wszystkich krawędziach jednego koloru, izomorficzny z G. Badanie, przy jakich mocach zbioru X ma miejsce podobna własność, wiąże się z tzw. liczbami kardynalnymi słabo zwartymi (p. np. Kuratowski i Mostowski [1], Erdös, Hajnal, Máté i Rado [1]).

Na zakończenie tego paragrafu wykażemy jeszcze pewną interesującą własność podziałową zbioru liczb naturalnych. Ze skończonego twierdzenia Ramsey'a wynika, że przy dowolnym podziale $\mathscr{P}_r(X) = A_1 \dot\cup \ldots \dot\cup A_t$, gdzie X jest dostatecznie dużym odcinkiem początkowym liczb naturalnych, istnieje zbiór $Y \subseteq X$ taki, że $|Y| \geqslant k$ oraz $\mathscr{P}_r(Y) \subseteq A_i$ dla pewnego $i \in \{1, \ldots, t\}$. Poniższe twierdzenie orzeka, iż na zbiór Y można narzucić dodatkowo ograniczenie $\min Y \leqslant |Y|$.

TWIERDZENIE 10.3 (Paris i Harrington [1]). *Dla dowolnych $k, r, t \in N$ istnieje liczba n o tej własności, że dla dowolnego $m \geqslant n$ i dowolnego pokolorowania $C\colon \mathscr{P}_r(\{1, \ldots, m\}) \to \{1, \ldots, t\}$ istnieje zbiór $Y \subseteq \{1, \ldots, m\}$ taki, że* $\min Y \leqslant |Y|$, *$|Y| \geqslant k$ oraz wszystkie r-elementowe podzbiory zbioru Y są tego samego koloru.*

Dowód. Zauważmy, że wystarczy pokazać własność, o której mowa w tezie twierdzenia, jedynie dla $m = n$, a stąd łatwo już wynika przypadek dowolnego $m \geqslant n$.

Ustalmy liczby k, r, t i przypuśćmy, że nie istnieje liczba n, o której mowa w tezie twierdzenia. Liczbę m będziemy nazywali *wymiarem pokolorowania* $C\colon \mathscr{P}_r(\{1, \ldots, m\}) \to \{1, \ldots, t\}$. Będziemy mówili, że pokolorowanie takie jest *kontrprzykładem*, jeśli nie istnieje żaden podzbiór $Y \subseteq \{1, \ldots, m\}$ taki, że funkcja $C \restriction \mathscr{P}_r(Y)$ jest stała, $|Y| \geqslant k$ i $\min Y \leqslant |Y|$.

Rozważmy drzewo $T = \langle X, \leqslant \rangle$, gdzie X jest zbiorem wszystkich kontrprzykładów, oraz

$$C \leqslant C' \Leftrightarrow C = C' \restriction \mathscr{P}_r(\{1, \ldots, m\}),$$

gdzie m oznacza wymiar kontrprzykładu C. Drzewo T jest nieskończone, jako że założyliśmy nieistnienie liczby n, o której mowa w tezie twierdzenia, a tym samym istnienie co najmniej jednego kontrprzykładu każdego wymiaru. Zauważmy, że

jeśli C jest kontrprzykładem wymiaru m, to $C \upharpoonright \mathscr{P}_r(\{1, \ldots, m'\})$ jest kontrprzykładem dla dowolnego $m' \leqslant m$. Wynika stąd, że w drzewie T każdy bezpośredni następnik kontrprzykładu C wymiaru m jest kontrprzykładem wymiaru $m+1$ i w konsekwencji liczba takich bezpośrednich następników jest skończona (nie przekracza $t^{\binom{m}{r-1}}$. Z lematu Königa wnioskujemy o istnieniu gałęzi nieskończonej $C_1 < C_2 < \ldots$ (C_i jest wymiaru i). Zdefiniujmy pokolorowanie $C: \mathscr{P}_r(N) \to \{1, \ldots, t\}$ następująco: $C(A) = C_i(A)$ dla $i \geqslant \max A$. Na mocy nieskończonego twierdzenia Ramsey'a istnieje zbiór nieskończony $Y \subseteq N$ taki, że funkcja $C \upharpoonright \mathscr{P}_r(Y)$ jest stała. Niech $a = \min Y$, rozważmy m takie, że $|Y \cap \{1, \ldots, m\}| \geqslant \max(a, k)$ i oznaczmy $H = Y \cap \{1, \ldots, m\}$. Mamy $\min H = a \leqslant |H|$, $|H| \geqslant k$ oraz funkcja $C \upharpoonright \mathscr{P}_r(H) = C_m \upharpoonright \mathscr{P}_r(H)$ jest stała. Lecz z drugiej strony, na mocy naszej konstrukcji, C_m jest kontrprzykładem. Tak więc przypuszczenie o nieistnieniu liczby n dla danych k, r, t doprowadziło nas do sprzeczności. Dowód jest tym samym zakończony. □

Warto tu wspomnieć, że fakt iż w dowodzie twierdzenia Parisa–Harringtona używaliśmy metod „infinitarnych" (lemat Königa) nie jest bynajmniej przypadkowy. Głęboki wynik Parisa i Harringtona [1] mówi, że twierdzenie to nie może być wykazane w arytmetyce Peano, a więc nie ma dowodu „elementarnego" (ciekawe, że dla każdego ustalonego r taki dowód istnieje; jednak dla różnych r odpowiednie dowody są tak „różne", że nie dają się one wszystkie zebrać w jeden elementarny dowód całego twierdzenia).

Oznaczmy przez $H(k, r, t)$ najmniejszą z liczb n, o której mowa w tezie twierdzenia Parisa–Harringtona. Okazuje się (Paris i Harrington [1], p. też Smoryński [1] i Mills [2]), że liczby $H(k, r, t)$ rosną nieporównanie szybciej ze wzrostem argumentów niż jakiekolwiek funkcje, z którymi mamy zwykle do czynienia w matematyce (np. analogiczne liczby Ramsey'a). Można wykazać, że funkcja $f(n) = H(n+1, n, n)$ rośnie zbyt szybko, by mogła być zdefiniowana za pomocą dodawania, mnożenia i indukcji (fakt ten ściśle się zresztą wiąże z niezależnością twierdzenia 10.3 od arytmetyki Peano).

Zadania

1. W ciągu jednego miesiąca (30 dni) pewien zespół pracowników zmontował $n < 50$ samochodów, przy czym codziennie montowano całkowitą i dodatnią liczbę samochodów. Udowodnić, że w pewnym okresie kolejnych dni zmontowano dokładnie 10 samochodów.

2. Udowodnić, że jeśli $n \geqslant R(m, m, m, m)$, to dowolna macierz zero-jedynkowa wymiaru $n \times n$ zawiera podmacierz główną (tzn. otrzymaną przez wybranie wierszy i kolumn o tych samych numerach), wymiaru $m \times m$ jednej z następujących czterech postaci:

$$\begin{bmatrix} * & & 0 \\ & \ddots & \\ 0 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 1 \\ & \ddots & \\ 1 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 1 \\ & \ddots & \\ 0 & & * \end{bmatrix}, \quad \begin{bmatrix} * & & 0 \\ & \ddots & \\ 1 & & * \end{bmatrix}.$$

Każda gwiazdka oznacza 0 lub 1, oraz każda z tych czterech macierzy zawiera nad i pod główną przekątną albo same zera albo same jedynki.

3. Udowodnić, że $R_r(q_1, \ldots, q_t) = R_r(q_{\sigma(1)}, \ldots, q_{\sigma(t)})$ dla dowolnej permutacji σ zbioru $\{1, \ldots, t\}$.

4. Udowodnić następujące twierdzenie Turàna [1]: Niech $M(n, k)$ oznacza maksymalną liczbę krawędzi w grafie o n wierzchołkach nie zawierającym grafu K_k jako podgrafu. Niech r będzie liczbą taką, że $1 \leqslant r \leqslant k-1$ oraz $n = t(k-1)+r$. Wówczas

$$M(n, k) = \frac{k-2}{2(k-1)}(n^2 - r^2) + \binom{r}{2}.$$

Wskazówka: Zastosować indukcję względem t.

5. Danych jest n liczb całkowitych $m_1, \ldots, m_n$. Udowodnić, że istnieją liczby p, q takie, że $1 \leqslant p < q \leqslant n$ oraz suma $n_{p+1} + n_{p+2} + \ldots + n_q$ jest podzielna przez n.

6. Udowodnić, że w grupie $n > 1$ osób są zawsze dwie, które mają w tej grupie jednakową liczbę znajomych.

7. Udowodnić, że dla dowolnych 52 liczb całkowitych istnieją dwie, których suma lub różnica jest podzielna przez 100.

8. Udowodnić, że przy dowolnym pokolorowaniu krawędzi grafu K_6 (K_7) na dwa kolory, istnieją co najmniej dwa (trzy) trójkąty jednokolorowe.

9. Udowodnić, że

$$R_r(q_1, \ldots, q_t) \leqslant R_{r-1}(p_1, \ldots, p_t),$$

gdzie $p_i = R_r(q_1, \ldots, q_{i-1}, q_i - 1, q_{i+1}, \ldots, q_t)$. W szczególności

$$R(q_1, \ldots, q_t) \leqslant R(q_1 - 1, q_2, \ldots, q_t) + R(q_1, q_2 - 1, q_3, \ldots, q_t) + \ldots + R(q_1, q_2, \ldots, q_t - 1) - t + 1.$$

10. Udowodnić następujące wzmocnienie nierówności (2.1). Jeśli obie liczby $R(m-1, n)$, $R(m, n-1)$ są parzyste, to

$$R(m, n) < R(m-1, n) + R(m, n-1).$$

11. (Erdös i O'Neil [1]). Udowodnić, że dla dowolnych liczb l_i, k_i, $1 \leqslant i \leqslant t$, takich, że $l_i \geqslant r \geqslant k_i > 0$ dla $1 \leqslant i \leqslant t$, istnieje liczba m o następującej własności:

Jeśli $|X| \geqslant m$ oraz $\mathscr{P}_r(X) = A_1 \cup \ldots \cup A_t$, to istnieje $i \in \{1, \ldots, t\}$ oraz zbiór $Y \subseteq X$ taki, że

(i) $|Y| \geqslant l_i$,

(ii) dla każdego $Z \in \mathscr{P}_{k_i}(Y)$ istnieje $T \in A_i$ takie, że $Z \subseteq T$.

Oznaczając przez $N_r(l_1, k_1; l_2, k_2; \ldots; l_t, k_t)$ najmniejszą z liczb m o tej własności udowodnić, że

(a) $N_r(r, k_1; l, k_2) = N_r(l, k_1; r, k_2) = l$,

(b) $N_r(l_1, k_1; l_2, k_2) \leqslant N_{r-1}(p_1, k_1 - 1; p_2, k_2 - 1) + 1$, gdzie $p_1 = N_r(l_1 - 1, k_1; l_2, k_2)$, $p_2 = N_r(l_1, k_1; l_2 - 1, k_2)$,

(c) Jeśli $k_1 + k_2 = r + 1$, to

$$N_r(l_1, k_1; l_2, k_2) = l_1 + l_2 - k_1 - k_2 + 1,$$

(d) Jeśli $k_1 + k_2 \leqslant r$, to

$$N_r(l_1, k_1; l_2, k_2) = \max(l_1, l_2).$$

12. Udowodnić, że jeśli krawędzie grafu K_n pokolorujemy dwoma kolorami, czerwonym i niebieskim, tak że do i-tego wierzchołka ($i = 1, \ldots, n$) dochodzi dokładnie r_i czerwonych krawędzi, to liczba jednokolorowych (czerwonych lub niebieskich) trójkątów jest równa

$$\Delta = \binom{n}{3} - \frac{1}{2}\sum_{i=1}^{n} r_i(n-1-r_i).$$

Wskazówka: Każdy trójkąt, który nie jest jednokolorowy, ma dokładnie dwa wierzchołki, w których spotykają się krawędzie różnych kolorów.

Wyprowadzić stąd oszacowanie

$$\Delta \geqslant \binom{n}{3} - \left\lfloor \frac{n}{2} \left\lfloor \left(\frac{n-1}{2}\right)^2 \right\rfloor \right\rfloor.$$

13. Wykazać, nie korzystając ze wzoru Stirlinga, że

$$2^{2n}/(2\sqrt{n}) < \binom{2n}{n} < 2^{2n}/\sqrt{2n}.$$

Wskazówka: Niech $P = \dfrac{1\cdot 3\cdot 5\cdot \ldots \cdot(2n-1)}{2\cdot 4\cdot 6\cdot \ldots \cdot 2n}$. Mamy

$$P = \frac{(2n)!}{2^{2n}(n!)^2} = \binom{2n}{n}/2^{2n}$$

oraz $P^2 < 1/(2n+1)$.

14. (Erdős). Udowodnić, że

$$R_3(n, n) \geqslant n2^{(n^2/6)-(n/2)}\left(\frac{3\sqrt{2}}{e} - o(1)\right).$$

Znaleźć podobne oszacowanie na $R_4(n, n)$.

15. (Erdős i Spencer [1]). Uzasadnić i uzupełnić szczegóły następującego probabilistycznego dowodu twierdzenia 2.2: Niech C będzie losowo wybranym podzbiorem zbioru X oraz niech $A \in \mathscr{X}$. Dla dowolnego $x \in X$ mamy $\mathrm{Prob}(x \in C) = \frac{1}{2}$, stąd $\mathrm{Prob}(A \subseteq C) = 2^{-n}$, $\mathrm{Prob}(A \subseteq X \setminus C) = 2^{-n}$. Zatem wartość oczekiwana liczby zbiorów $A \in \mathscr{X}$ takich, że $A \subseteq C \vee A \subseteq X \setminus C$ wynosi $|\mathscr{X}|2^{-n+1}$. Z założeń twierdzenia wynika, że ta wartość oczekiwana jest nie mniejsza niż 1. Stąd $|\mathscr{X}| \geqslant 2^{n-1}$.

16. (Folkman). Wykazać, że dla dowolnych grafów G, H istnieje taki graf K, że przy każdym pokolorowaniu jego wierzchołków na czerwono i niebiesko powstaje podgraf indukowany izomorficzny z G o wszystkich wierzchołkach czerwonych lub też podgraf indukowany izomorficzny z H o wszystkich wierzchołkach niebieskich.

17. Udowodnić, że dla dowolnych grafów $G_1, \ldots, G_t$ istnieje graf K taki, że $K \to (G_1, \ldots, G_t)$ (znaczenie tego symbolu jest analogiczne do znaczenia symbolu $K \to (G, H)$ wyjaśnionego w dowodzie twierdzenia Deubera, § 3).

18. Skonstruować graf K taki, że $K \to (C_4, C_4)$, gdzie C_k jest cyklem długości k.

19. (Gerencsér i Gyárfás [1]). Udowodnić, że dla $k \geqslant l$ liczba Ramsey'a $r(P_k, P_l)$ jest równa $k + \lfloor (l+1)/2 \rfloor$. Przez P_k oznaczamy tu drogę (elementarną) o k wierzchołkach.

20. (Harary [1]). Udowodnić, że

$$r(K_{1,m}, K_{1,n}) = \begin{cases} m+n-1, & \text{jeśli obie liczby } m, n \text{ są parzyste,} \\ m+n, & \text{w przeciwnym przypadku.} \end{cases}$$

Przez $K_{1,m}$ oznaczamy tu graf dwudzielny o $m+1$ wierzchołkach i m krawędziach łączący jeden z wierzchołków ze wszystkimi pozostałymi.

21. (Harary i Hell). Niech $\vec{K}_m$ oznacza graf zorientowany o m wierzchołkach, w którym każde dwa wierzchołki x, y są połączone dwoma krawędziami $\langle x, y\rangle$, $\langle y, x\rangle$. Niech D_1, D_2 będą dwoma grafami zorientowanymi. Niech liczba $r(D_1, D_2)$ będzie zdefiniowana jako najmniejsze m takie, że przy każdym pokolorowaniu krawędzi grafu $\vec{K}_m$ dwoma kolorami, czerwonym i niebieskim, powstaje podgraf czerwony izomorficzny z D_1 lub podgraf niebieski izomorficzny z D_2. Udowodnić, że $r(D_1, D_2)$ istnieje wtedy i tylko wtedy, gdy co najmniej jeden z grafów D_1, D_2 nie zawiera cykli.

22. Czy prawdziwe jest twierdzenie: Jeśli $N = A_1 \cup A_2$, to A_1 lub A_2 zawiera nieskończony postęp arytmetyczny?.

23. Udowodnić, że $W(2, k) \geqslant \sqrt{(k-1)2^k}$.

Wskazówka: Skorzystać z twierdzenia 3.2.

24 (Simmons). Korzystając z twierdzenia van der Waerdena udowodnić, że przy każdym pokolorowaniu płaszczyzny na skończoną liczbę kolorów istnieje dowolnie mały i dowolnie duży trójkąt równoboczny o wierzchołkach tego samego koloru.

25 (Berlekamp [1]). Niech q będzie potęgą liczby pierwszej, m liczbą pierwszą oraz a elementem pierwotnym w ciele $GF(p^m)$ (por. Dodatek). Niech

$$\mathrm{Tr}(x) = \sum_{i=0}^{m-1} x^{q^i}.$$

Dla każdego $x \in GF(q)$ oznaczmy

$$S_x = \{s\colon\ 0 \leqslant s < k(q^m-1) \wedge \mathrm{Tr}(a^s) = x\}.$$

Udowodnić, że $\bigcup_{x \in GF(q)} S_x = \{0, 1, 2, \ldots, k(q^m-1)-1\}$ i że żaden ze zbiorów S_x nie zawiera postępu arytmetycznego długości większej niż k. Wyprowadzić stąd dolne oszacowanie na liczby $W(t, k)$.

26. Wykazać, że dla dowolnego $n \geqslant 1$ istnieje najmniejsza liczba $P(n)$ taka, że ilekroć $m \geqslant P(n)$ i $\{2, 3, \ldots, P(n)\} = A_1 \cup \ldots \cup A_n$, to któryś ze zbiorów A_i zawiera liczby a, b, c (niekoniecznie różne) takie, że $a \cdot b = c$. Udowodnić, że

$$2^{(3^n+1)/2-1}+1 \leqslant P(n) \leqslant 2^{\lfloor n!e \rfloor}.$$

27. Korzystając z równości $S(4) = 45$ wykazać, że

$$S(n) \geqslant \frac{1}{2}\left(\frac{89}{81}3^n+1\right)$$

dla $n \geqslant 4$.

28. Niech $g(l)$ będzie najmniejszą liczbą zbiorów wolnych od sum, na które można rozłożyć $\{1, \ldots, l\}$. Wykazać, że $g(l) < \ln l$ dla dostatecznie dużych l.

29. Znaleźć podział zbioru $\{1, 2, \ldots, 13\}$ na 3 podzbiory wolne od sum $(\frac{1}{2}(3^3+1)-1 = 13$, wystarczy zatem zastosować konstrukcję z lematu 5.2).

30. Rodzina $\mathfrak{M} \subseteq \mathscr{P}(X)$ jest wolna od sum, jeśli nie istnieją trzy różne zbiory $A, B, C \in \mathfrak{M}$ takie, że $A \cup B = C$. Wykazać, że jeśli $|X| = n$, to $\mathscr{P}(X)$ można rozłożyć na $\lfloor n/2 \rfloor + 1$ podrodzin wolnych od sum.

Wskazówka: Rozważyć następujący podział zbioru $\{1, \ldots, n\}$:

$$C_1 = \{1, 3, 7, \ldots, 2^j-1, \ldots\},$$
$$C_i = \{2(i-1), 4(i-1)+1, 8(i-1)+3, \ldots, 2^j(i-1)+ +2^{j-1}-1, \ldots\}, \quad i = 2, 3, \ldots, \lfloor n/2 \rfloor + 1,$$

a następnie określić

$$\mathscr{P}(X) = A_1 \cup \ldots \cup A_{\lfloor n/2 \rfloor+1}, \text{ gdzie } A_i = \{Y \subseteq X\colon |Y| \in C_i\}.$$

31. Podać przykład nieskończonego zbioru liczb naturalnych wolnego od sum.

32. (Abbott i Hanson [1]). Niech (S_k) będzie następującym układem $\binom{k-1}{2}$ równań z $\binom{k}{2}$ niewiadomymi:

$$x_{i,j} + x_{j,j+1} = x_{i,j+1}, \quad 1 \leqslant i < j \leqslant k-1.$$

Udowodnić, że dla każdego $n \geq 1$ istnieje największa liczba $f_k(n)$, dla której istnieje podział $\{1, \ldots, f_k(n)\} = A_1 \cup \ldots \cup A_n$ taki, że żaden ze zbiorów A_i nie zawiera liczb x_{ij}, $1 \leq i < j \leq k$ będących rozwiązaniem układu (S_k). Wykazać, że $f_k(n) \leq R(k_1, \ldots, k_n) - 2$, $k_1 = \ldots = k_n = k$.

33. Niech $\langle G, + \rangle$ będzie grupą o m elementach i niech $G \setminus \{0\} = A_1 \dot\cup \ldots \dot\cup A_n$ będzie podziałem na zbiory wolne od sum takie, że $A_i = -A_i$ $(-A_i = \{-a\colon a \in A_i\})$. Udowodnić, że $R^{(n)}(3) \geq m+1$.

34. Niech Z_4 będzie grupą reszt modulo 4. Sprawdzić, że

$$(Z_4 \oplus Z_4) \setminus \{\langle 0, 0 \rangle\} = S_1 \cup S_2 \cup S_3,$$

gdzie

$$S_1 = \{\langle 0, 2\rangle, \langle 1, 0\rangle, \langle 3, 0\rangle, \langle 1, 1\rangle, \langle 3, 3\rangle\},$$
$$S_2 = \{\langle 2, 0\rangle, \langle 0, 1\rangle, \langle 0, 3\rangle, \langle 1, 3\rangle, \langle 3, 1\rangle\},$$
$$S_3 = \{\langle 2, 2\rangle, \langle 2, 1\rangle, \langle 2, 3\rangle, \langle 1, 2\rangle, \langle 3, 2\rangle\}$$

jest podziałem na zbiory wolne od sum takie, że $S_i = -S_i$. Korzystając z poprzedniego zadania i lematu 5.2 udowodnić, że $R(3, 3, 3) = 17$.

35. Udowodnić, że $R(3, 4) \leq 9$.

Wskazówka: Pokolorowanie krawędzi grafu K_9 takie, że do każdego wierzchołka dochodzą trzy czerwone i pięć niebieskich krawędzi jest niemożliwe wobec nieparzystości liczb 3, 5, 9; przy każdym innym pokolorowaniu pojawia się natomiast czerwony trójkąt lub niebieski graf K_4. Wykazać, że $R(3, 4) = 9$ przez pokolorowanie krawędzi $\{i, j\}$ grafu K_8 o wierzchołkach $0, 1, \ldots, 7$ na czerwono, jeśli $i-j \equiv 4, 1, 7 \pmod 8$, i na niebiesko w pozostałych przypadkach.

36. Korzystając z wyniku poprzedniego zadania udowodnić, że $R(4, 4) \leq 18$. Wykazać, że $R(4, 4) = 18$ kolorując krawędź $\{i, j\}$ grafu K_{17} o wierzchołkach $0, 1, \ldots, 16$ na czerwono, jeśli $i-j \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17}$, i na niebiesko w przeciwnym przypadku.

37. Korzystając z zadania 4 udowodnić, że $R(3, 5) \leq 14$. Wykazać równość $R(3, 5) = 14$ przez pokolorowanie krawędzi $\{i, j\}$ grafu K_{13} o wierzchołkach $0, 1, \ldots, 12$ na czerwono, jeśli $i-j \equiv \pm 1, \pm 5 \pmod{13}$, i na niebiesko w przeciwnym przypadku.

38 (Spencer [1]). Udowodnić następujące wzmocnienie twierdzenia van der Waerdena: Dla wszelkich $k, t > 1$ oraz każdego ciągu $\varepsilon_0, \ldots, \varepsilon_{k-1} \in \{0, 1\}$ istnieje zbiór liczb naturalnych A taki, że dla dowolnego podziału $A = A_1 \cup \ldots \cup A_t$ istnieje $i \in \{1, \ldots, t\}$ oraz postęp arytmetyczny $\beta_0, \ldots, \beta_{k-1}$ taki, że $\{\beta_i\colon 0 \leq i \leq k-1 \wedge \varepsilon_i = 1\} \subseteq A_i$ oraz $\beta_i \notin A$ dla i takich, że $\varepsilon_i = 0$.

39. Udowodnić, że otoczka wypukła dowolnego skończonego zbioru P punktów płaszczyzny jest wielokątem wypukłym o wierzchołkach należących do P.

40. Sprawdzić, że $N_3 = 3$, $N_4 = 5$, $N_5 = 9$ (por. § 9).

41. Przeprowadzić dowód twierdzenia 10.2 dla dowolnych $t, r \in N$.

42. Wykazać, że istnieje rodzina $\mathscr{F} \subseteq \mathscr{P}(N)$ taka, że $|\mathscr{F}| = 2^{\aleph_0}$ oraz dla dowolnych skończonych ciągów $A_1, \ldots, A_n \in \mathscr{F}$ oraz $\varepsilon_1, \ldots, \varepsilon_n \in \{0, 1\}$ zbiór $A_1^{\varepsilon_1} \cap \ldots \cap A_n^{\varepsilon_n}$ jest niepusty $(A_i^0 = A_i,\ A_i^1 = N \setminus A_i)$.

43. Udowodnić, że każdy nieskończony ciąg liczb rzeczywistych zawiera podciąg (nieskończony) stały lub ściśle monotoniczny.

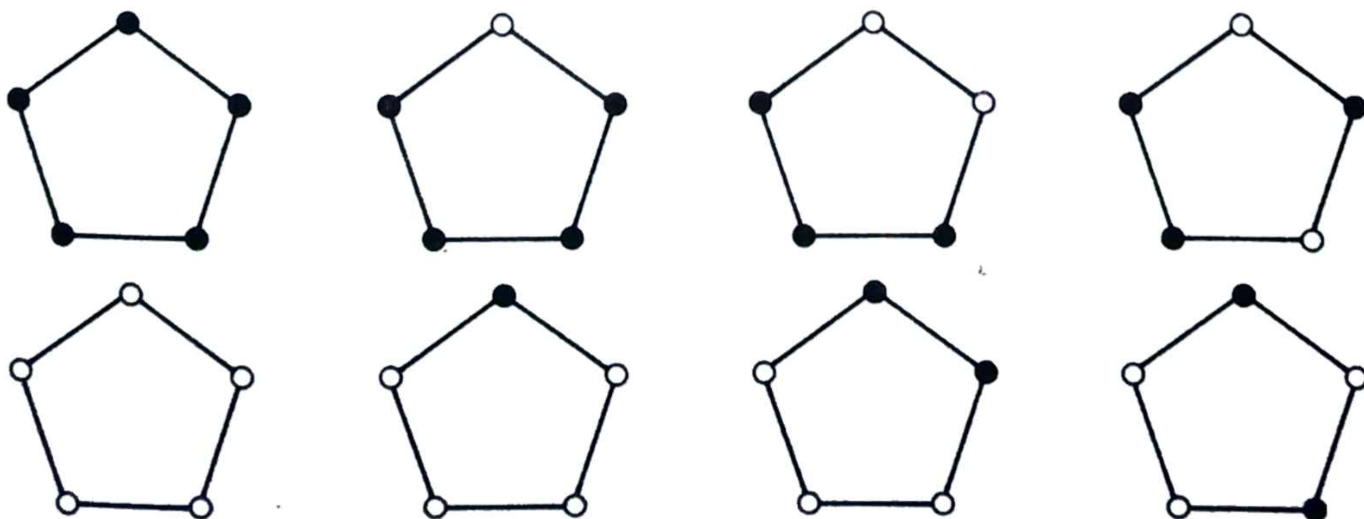
ZLICZANIE ORBIT GRUPY DZIAŁAJĄCEJ NA ZBIORZE

Często napotykany w zastosowaniach kombinatoryki problem polega na wyznaczaniu liczby „istotnie różnych" obiektów o zadanych własnościach, przy czym dwa obiekty uznamy za „takie same", jeżeli można je nawzajem z siebie otrzymać poprzez zastosowanie pewnych operacji określonych warunkami zadania.

Przypuśćmy, dla przykładu, że na stole leżą dwie kostki do gry o jednakowym rozmiarze i wyglądzie. Uznamy je za „takie same", jeżeli po wyrzuceniu ich z kubka na stół nie będziemy w stanie powiedzieć, która z nich leżała po lewej, a która po prawej stronie. Wobec powyższego operacjami dopuszczonymi w naszym problemie będą wszelkie możliwe obroty kostki w przestrzeni trójwymiarowej.

Klasycznego przykładu naszego zadania dostarcza tak zwany „problem naszyjników". Dysponujemy zapasem białych i czarnych paciorków, które nawlekamy na sznurek i łączymy go w pętlę. Ile możemy nawlec „istotnie różnych" naszyjników o n paciorkach? Dokładniej, malujemy wierzchołki n-kąta foremnego na biało i czarno. Można to oczywiście zrobić na 2^n sposobów. Dwa pokolorowania uznamy za różne, jeżeli nie istnieje przekształcenie z grupy symetrii D_n n-kąta foremnego, które jedno z tych pokolorowań przekształca na drugie. Pytamy o liczbę różnych pokolorowań. Łatwo jest narysować wszystkie takie naszyjniki dla małych wartości n. Przypuśćmy, że $n = 5$. Wszystkie 8 różnych naszyjników pokazano na rys. 25.

Zauważmy, że grupa przekształceń identyfikujących pokolorowania i odpo-



Rys. 25. Wszystkie istotnie różne naszyjniki dla $n = 5$

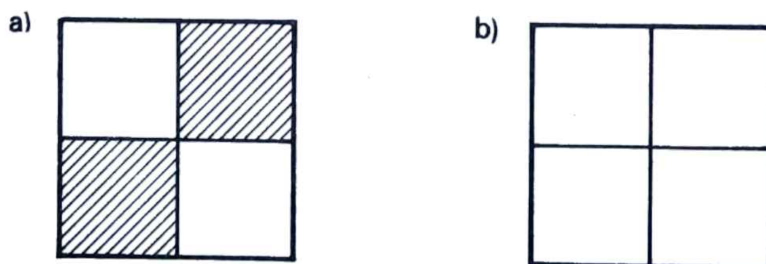
wiedź na nasze pytanie natychmiast się zmieni (jak?), jeżeli założymy, że naszyjniki mają w pewnym wyróżnionym miejscu zapięcie.

Uproszczona wersja zadania o naszyjnikach, w której dopuszczalnymi przekształceniami były tylko obroty, a nie dowolne symetrie pięciokąta foremnego, była już rozwiązana w rozdziale 2, § 5. Tutaj jednakże pokażemy metody pozwalające na znalezienie liczby „różnych obiektów", o ile tylko obiekty te będą utożsamiane za pomocą operacji tworzących grupę. Podstawowym narzędziem do tego celu będzie twierdzenie zwane „lematem Burnside'a", opisane w pierwszym paragrafie. Pozostałe wyniki tego rozdziału można potraktować jako wnioski z tego twierdzenia, albo jako jego równoważne formy dostosowane do specyficznych potrzeb. Należy do nich w pierwszym rzędzie twierdzenie Pólya, w którym do odnajdywania liczby „różnych" funkcji używa się wielomianu zwanego indeksem cyklowym, a który zależy od działania grupy na wspólnej dziedzinie rozpatrywanego zbioru funkcji. Metodom odnajdywania indeksów cyklowych poświęcamy następny paragraf. Na zakończenie pokażemy, jak używać tak zwanych wag. Pozwoli to na wyodrębnienie pewnych podzbiorów z badanych zbiorów funkcji. Będziemy mogli, na przykład, odnaleźć liczbę „różnych" naszyjników o k paciorkach białych i $n-k$ paciorkach czarnych.

§ 1. Lemat Burnside'a

Wspomnieliśmy powyżej, że będziemy rozważali te zadania, w których operacje identyfikujące obiekty tworzą grupę. Grupa ta jest oczywiście wyznaczona przez warunki zadania. Zilustrujemy tę zależność od problemu kombinatorycznego na jeszcze jednym przykładzie.

Z okazji Bardzo Ważnych Mistrzostw Szachowych przyozdabiamy miasto emblematami szachownicy, takimi jak na rys. 26(a).



Rys. 26. Emblematy szachownicy

W teren udała się ekipa niezbyt dokładnie poinformowanych malarzy i zamalowywuje uprzednio przygotowane schematy (rys. 26(b)) w sposób zupełnie przypadkowy. Żywotnie interesują nas szanse odnalezienia emblematów pomalowanych właściwie. Otóż, jeżeli schemat znajdował się na ścianie domu, to grupa dopuszczalnych przekształceń składa się wyłącznie z identyczności; jeżeli był to

stojak obciągnięty przejrzystym materiałem, to możemy go obrócić jeszcze wokół pionowej osi, a więc grupa ma dwa elementy; jeżeli schemat był na kwadratowej desce, to grupą jest C_4 — grupa obrotów kwadratu; dla szklanej kwadratowej płyty grupą będzie grupa D_4 symetrii kwadratu; w końcu grupa S_4 wszystkich permutacji czterech elementów pojawi się wtedy, gdy schemat będzie się składał z czterech oddzielnych płytek takich jak kafelki glazury.

W dalszym ciągu udowodnimy twierdzenia pozwalające odnaleźć poszukiwane szanse w każdym z opisanych przypadków. Uprzednio jednakże, dla uściślenia sformułowań, wprowadzimy pewien formalizm.

Będziemy mówili, że grupa G (zapisywana multyplikatywnie) *działa na zbiorze* A, jeżeli jest dane przekształcenie z $G \times A$ w A, w którym obrazem pary $\langle \alpha, a \rangle$, $\alpha \in G$, $a \in A$, jest element zbioru A oznaczany przez αa, i które ma następujące własności: $\varepsilon a = a$ oraz $(\alpha\beta)a = \alpha(\beta a)$, gdzie ε jest jedynką grupy G, α, $\beta \in G$ i $a \in A$. Elementy grupy G będą też nazywane *operatorami*, a o zbiorze A wraz z działającą na nim grupą G będziemy też mówili, nadużywając nieco języka, jako o *G-zbiorze*.

Opisane powyżej przykłady są przykładami G-zbiorów, gdzie zbiorami A są odpowiednio: zbiór kostek do gry (tzn. zbiór funkcji różnowartościowych ze zbioru ścian danego sześcianu w $\{1, 2, 3, 4, 5, 6\}$), zbiór pokolorowań wierzchołków n-kąta foremnego i zbiór pokolorowań szachownicy o czterech polach, a grupy zostały opisane uprzednio. Każda podgrupa grupy wszystkich przekształceń różnowartościowych zbioru A na siebie dostarcza przykładu działania grupy na zbiorze, jeżeli przyjmiemy $\alpha a = \alpha(a)$, $a \in A$. Inny przykład G-zbioru otrzymamy biorąc dowolną grupę G, dowolny zbiór A i definiując $\alpha a = a$, dla każdego $\alpha \in G$ i każdego $a \in A$. Każda grupa działa na zbiorze swoich elementów mnożąc je z lewej strony. Inne działanie grupy G na zbiorze G otrzymamy odwzorowując parę $\langle \alpha, \gamma \rangle \in G \times G$ na $\alpha\gamma\alpha^{-1}$.

Zauważmy, że analogicznie do działania grupy G na zbiorze A z lewej strony możemy zdefiniować działanie G na A ze strony prawej. Jednakże, jeżeli oznaczymy przez $a * \alpha$ wynik działania z prawej operatora $\alpha \in G$ na element $a \in A$, to przyjmując $\alpha^{-1}a = a * \alpha$, lub równoważnie $\alpha a = a * \alpha^{-1}$, określimy działanie G na A ze strony lewej. Podobnie lewostronne działanie wyznacza działanie prawostronne. Szczegóły pozostawiamy do sprawdzenia Czytelnikowi.

Niech a będzie elementem G-zbioru A. Przez Ga oznaczymy zbiór $\{\alpha a \colon \alpha \in G\}$, który nazwiemy *G-orbitą* elementu a (lub też *orbitą elementu a przy działaniu grupy G*). Jeżeli $Ga = \{a\}$, to a nazywa się *punktem stałym* względem G.

LEMAT 1.1. *Niech A będzie G-zbiorem. Rodzina orbit* $\{Ga \colon a \in A\}$ *jest podziałem zbioru A na parami rozłączne niepuste zbiory dające w sumie cały zbiór A.*

Dowód. Zauważmy, że $\bigcup \{Ga \colon a \in A\} = A$ i wszystkie orbity są niepuste, gdyż $a = \varepsilon a \in Ga$. Jeżeli $c \in Ga \cap Gb$, to istnieją α i β należące do G takie, że $c = \alpha a = \beta b$. Zatem $a = \alpha^{-1}\beta b$, a więc $Ga = G(\alpha^{-1}\beta b) = (G\alpha^{-1}\beta)b = Gb$. □

Nasze oryginalne zadanie można teraz uściślić następująco. Dane jest działanie

grupy G na zbiorze A. Znaleźć liczbę G-orbit. Będziemy w dalszym ciągu stale zakładali, choć nie było to potrzebne w definicjach, że zarówno grupa G jak i G-zbiór są skończone.

Oznaczmy przez G_a *stabilizator* elementu a, to znaczy zbiór $\{\alpha \in G\colon \alpha a = a\}$. Łatwo zauważyć, że jeżeli $\alpha, \beta \in G_a$, to także $\alpha^{-1}\beta \in G_a$. Zatem stabilizator jest podgrupą. Ponadto dla dowolnych $\beta, \gamma \in G$ mamy oczywiście $\beta G_a a = \{\beta a\}$, natomiast $\beta a = \gamma a$ pociąga za sobą $\gamma^{-1}\beta \in G_a$. Wobec tego odwzorowanie $\beta G_a \mapsto \beta a$ ustala równoliczność zbioru $\{\beta G_a\colon \beta \in G\}$ prawostronnych warstw grupy G względem stabilizatora G_a i orbity Ga. Ponieważ, jak dobrze wiadomo, rząd grupy jest iloczynem rzędu podgrupy przez liczbę warstw względem tej podgrupy, więc udowodniliśmy następujący lemat.

LEMAT 1.2. *Jeżeli A jest G-zbiorem i $a \in A$, to*

$$|G| = |G_a| \cdot |Ga|. \quad \square$$

W szczególności wynika stąd, że wszystkie stabilizatory elementów tej samej orbity mają tyle samo elementów.

Poniższe twierdzenie, zwane „lematem Burnside'a", daje odpowiedź na problem sformułowany na początku tego rozdziału.

TWIERDZENIE 1.3 (lemat Burnside'a [1]). *Niech A będzie skończonym G-zbiorem. Liczba G-orbit, na które dzieli się zbiór A, jest równa*

$$\frac{1}{|G|} \sum_{\alpha \in G} \lambda(\alpha),$$

gdzie $\lambda(\alpha)$ oznacza liczność zbioru $\{a \in A\colon \alpha a = a\}$ punktów stałych operatora α.

Dowód. Niech zbiór $\{a_1, \ldots, a_m\}$ zawiera dokładnie po jednym elemencie z każdej orbity. Korzystając z lematu 1.2 i następującej po nim uwagi otrzymujemy

$$m \cdot |G| = \sum_{i=1}^{m} |Ga_i| \cdot |G_{a_i}| = \sum_{a \in A} |G_a|.$$

Zapisując inaczej ostatnią sumę i zmieniając porządek sumowania otrzymujemy

$$m \cdot |G| = \sum_{a \in A} \sum_{\alpha : \alpha a = a} 1 = \sum_{\alpha \in G} \sum_{a : \alpha a = a} 1 = \sum_{\alpha \in G} \lambda(\alpha),$$

skąd otrzymujemy żądany wynik dzieląc stronami przez $|G|$. $\square$

Skoro każdemu działaniu grupy G na zbiorze A z prawej strony odpowiada lewostronne działanie G na A, przy którym orbity są takie same, to z udowodnionego twierdzenia można natychmiast otrzymać „prawostronną" wersję lematu Burnside'a, co pozostawiamy Czytelnikowi.

Wróćmy do problemu naszyjników o pięciu paciorkach. Numerując wierzchołki pięciokąta foremnego możemy jego grupę symetrii D_5 przedstawić jako podgrupę grupy permutacji S_5 zbioru $\{1, 2, 3, 4, 5\}$. Grupa D_5 działa z prawej

strony na zbiorze pokolorowań, to znaczy funkcji f: $\{1, 2, 3, 4, 5\} \to \{$czarne, białe$\}$, w sposób następujący: Obrazem pokolorowania f przy działaniu operatora $\alpha \in D_5$ jest funkcja $f\alpha$, która na wierzchołku w przyjmuje wartość $f(\alpha w)$. (Czytelnik zechce sprawdzić, że zostało zdefiniowane działanie i że odpowiada ono kombinatorycznej treści zadania.) Łatwo zauważyć, że funkcja f jest punktem stałym dla α wtedy i tylko wtedy, gdy f przyjmuje tę samą wartość dla wszystkich elementów należących do jednego cyklu permutacji α.

W grupie D_5 jest jedna permutacja o pięciu cyklach, a mianowicie identyczność, i ma ona wobec tego w zbiorze pokolorowań 2^5 punktów stałych. Ponadto jest pięć permutacji o trzech cyklach — odbicia — i każda z nich ma 2^3 punktów stałych, oraz są cztery cykle długości pięć — nieidentycznościowe obroty — każdy z dwoma punktami stałymi. Z lematu Burnside'a wynika, że wszystkich orbit jest

$$\tfrac{1}{10}(1\cdot 2^5+5\cdot 2^3+4\cdot 2^1)=8.$$

Oznacza to, że na rys. 25 żaden naszyjnik nie został pominięty.

Przytoczmy jeszcze wynik Davisa [1], który użył lematu Burnside'a dla wyznaczenia liczby $T(n)$ nieizomorficznych turniejów rzędu n. *Turniejem rzędu* n nazywamy relację binarną T na n-elementowym zbiorze A taką, że dla żadnego $a\in A$ para $\langle a, a\rangle$ nie należy do T, i jeżeli $a\neq b$, to z dwóch par $\langle a, b\rangle$, $\langle b, a\rangle\in A\times A$ dokładnie jedna należy do T. Relację taką nazywamy turniejem, bo gdy przeprowadzimy rozgrywki pomiędzy n uczestnikami pewnych zawodów prowadzonych systemem „każdy z każdym" i przyjmiemy, że $\langle a, b\rangle\in T$ wtedy i tylko wtedy, gdy a wygrał z b, to otrzymamy turniej rzędu n. Turniej często jest reprezentowany za pomocą grafu zorientowanego o n wierzchołkach, w którym para wierzchołków a, b jest połączona zorientowaną krawędzią o początku w a i końcu w b wtedy i tylko wtedy, gdy $\langle a, b\rangle\in T$. Dwa turnieje T i T' nazwiemy *izomorficznymi*, jeżeli istnieje różnowartościowe przekształcenie φ ze zbioru wierzchołków T na zbiór wierzchołków T' takie, że $\langle a, b\rangle\in T$ wtedy i tylko wtedy, gdy $\langle\varphi(a), \varphi(b)\rangle\in T'$.

Jest jasne, że szukając liczby $T(n)$ możemy się ograniczyć do turniejów na zbiorze $\{1, \ldots, n\}$. Niech α należy do grupy S_n permutacji zbioru $\{1, \ldots, n\}$. Przyjmijmy $\alpha T=\{\langle\alpha a, \alpha b\rangle\colon \langle a, b\rangle\in T\}$ definiując tym, jak łatwo sprawdzić, działanie grupy S_n na zbiorze turniejów. Liczba $T(n)$ będzie dokładnie liczbą S_n-orbit w zbiorze turniejów na $\{1, \ldots, n\}$.

Aby zastosować lemat Burnside'a, musimy znaleźć liczby $\lambda(\alpha)$ tych turniejów, dla których $\alpha T=T$.

Przypomnijmy, że permutację $\alpha\in S_n$ nazywamy permutacją typu $d=$ $=1^{d_1}2^{d_2}\ldots n^{d_n}$, jeżeli w rozkładzie na cykle rozłączne ma ona d_i cykli długości i, $i=1, \ldots, n$. Mamy przy tym $d_1+2d_2+\ldots+nd_n=n$.

LEMAT 1.4. *Niech $\alpha\in S_n$ będzie permutacją typu $d=1^{d_1}2^{d_2}\ldots n^{d_n}$ działającą na zbiorze turniejów rzędu n. Jeżeli α ma cykl długości parzystej, to $\lambda(\alpha)=0$.*

W przeciwnym przypadku $\lambda(\alpha) = 2^{t(d)}$, *gdzie*

$$t(d) = \frac{1}{2}\Big(\sum_{i,j=1}^{n} [i, j] d_i d_j - \sum_{k=1}^{n} d_k\Big)$$

(*$[i, j]$ oznacza największą wspólną wielokrotność liczb i, j*).

Dowód. Niech α będzie permutacją z grupy S_n i T turniejem takim, że $\alpha T = T$. Przypuśćmy, że w rozkładzie α na cykle rozłączne występuje cykl $[a_1, a_2, \ldots, a_i]$. Grupa cykliczna (α) generowana przez α działa na zbiorze par $\{\langle a_s, a_t\rangle : 1 \leqslant s, t \leqslant i \wedge s \neq t\}$ i dzieli go na rodzinę (α)-orbit złożonych z takich par, dla których liczba $s-t \pmod i$ jest stałą różną od zera. Turniej T wraz z każdą parą zawiera oczywiście jej (α)-orbitę. Z dwóch par $\langle a_s, a_t\rangle$ i $\langle a_t, a_s\rangle$ dokładnie jedna należy do T, co oznacza, że dla żadnej pary $\langle s, t\rangle$, gdzie $s \neq t$, nie może zachodzić równość $s-t = t-s \pmod i$, lub równoważnie $2(s-t) = 0 \pmod i$. Jednakże jeżeli i jest parzyste, to dla spełnienia powyższej równości wystarczy przyjąć $s = i/2+1$ i $t = 1$. Zatem jeżeli α zawiera cykl długości parzystej, to $\lambda(\alpha) = 0$. Jeżeli natomiast i jest liczbą nieparzystą, to równość $2(s-t) = 0 \pmod i$ jest równoważna, przy naszych założeniach, $s = t$, co jest wykluczone. Uwzględniając, że $(\alpha)\langle a_s, a_t\rangle \subseteq T$ wtedy i tylko wtedy, gdy $(\alpha)\langle a_t, a_s\rangle \cap T = \emptyset$, oraz fakt, że wszystkich orbit jest $i-1$, widzimy, że turniej T na elementach cyklu $[a_1, a_2, \ldots, a_i]$ może być określony na $2^{(i-1)/2}$ sposobów.

Jeżeli $[a_1, a_2, \ldots, a_i]$ i $[b_1, b_2, \ldots, b_j]$ są cyklami rozłącznymi permutacji α, to łatwo zauważyć, że każda (α)-orbita pary $\langle a_s, b_t\rangle$, $1 \leqslant s \leqslant i$, $1 \leqslant t \leqslant j$, ma długość $[i, j]$. Skoro wszystkich takich par jest ij, to wszystkich (α)-orbit mamy $ij/[i, j] = (i, j)$. (Przypomnijmy, że (i, j) oznacza największy wspólny dzielnik liczb i, j.) Rozumując jak wyżej widzimy, że turniej T na elementach cykli $[a_1, a_2, \ldots, a_i]$ i $[b_1, b_2, \ldots, b_j]$ jest określony przez podanie zbioru (α)-orbit postaci $(\alpha)\langle a_s, b_t\rangle$, które są w nim zawarte. A więc mamy $2^{(i,j)}$ możliwości. Biorąc teraz pod uwagę, że permutacja α jest typu $1^{d_1}2^{d_2} \ldots n^{d_n}$, gdzie $d_2 = d_4 = \ldots = 0$, otrzymujemy z powyższego, iż wszystkich turniejów T takich, że $\alpha T = T$ jest $2^{t(d)}$, gdzie

$$t(d) = \sum_{i=1}^{n} \frac{d_i(i-1)}{2} + \sum_{i=1}^{n} \binom{d_i}{2}[i, i] + \sum_{i,j:\, 1 \leqslant i < j \leqslant n} d_i d_j [i, j] =$$

$$= \sum_{i=1}^{n} \frac{d_i(i-1)}{2} + \sum_{i=1}^{n} \frac{d_i^2}{2} i - \sum_{i=1}^{n} \frac{d_i}{2} i + \frac{1}{2} \sum_{i,j:i \neq j} d_i d_j [i, j].$$

Grupując drugą sumę z czwartą i pierwszą z trzecią natychmiast otrzymujemy, że

$$t(d) = \frac{1}{2} \sum_{i,j=1}^{n} [i, j] d_i d_j - \sum_{k=1}^{n} d_k. \ \square$$

Twierdzenie 1.5 (Davis [1]). *Liczba $T(n)$ nieizomorficznych turniejów rzędu*

n jest równa

$$\sum_d \frac{2^{t(d)}}{\prod_i i^{d_i} d_i!},$$

gdzie $t(d)$ *zostało określone w lemacie* 1.4, *a sumowanie rozciąga się po wszystkich rozwiązaniach w nieujemnych liczbach całkowitych równania*

$$d_1 + 3d_3 + 5d_5 + \ldots = n.$$

Dowód. Jak wiadomo (zob. twierdzenie 1.4.2) wszystkich permutacji typu $d = 1^{d_1} 2^{d_2} \ldots n^{d_n}$ jest

$$\frac{n!}{1^{d_1} d_1! 2^{d_2} d_2! \ldots n^{d_n} d_n!}.$$

Wobec tego, uwzględniając nasz wynik z poprzedniego lematu, z lematu Burnside'a otrzymujemy

$$T(n) = \frac{1}{n!} \sum_{\alpha \in S_n} \lambda(\alpha) = \sum_d \frac{2^{t(a)}}{1^{d_1} d_1!\, 2^{d_2} d_2! \ldots n^{d_n} d_n!},$$

gdzie sumowanie przebiega po zbiorze określonym w tezie twierdzenia. □

Następująca tablica wartości $T(n)$ pochodzi z książki Moona [1] (pierwszych osiem wartości było policzonych przez Davisa).

n	$T(n)$
1	
2	1
3	2
4	4
5	12
6	56
7	456
8	6 880
9	191 536
10	9 733 056
11	903 753 248
12	154 108 311 168

§ 2. Orbity grup działających na zbiorach funkcji

W kombinatorycznych zastosowaniach zazwyczaj wygodniejsze w użyciu od lematu Burnside'a są pewne jego konsekwencje pochodzące w zasadzie od Pólya, de Bruijna i Redfielda. Twierdzenia te dają efektywne metody przeliczania dla szerokiej klasy problemów.

Rozpoczniemy od przykładu. Rozważamy niezorientowane grafy o n wierzchołkach. Grafy $\Gamma = \langle V, E\rangle$ i $\Gamma' = \langle V', E'\rangle$ będziemy uważali za równoważne, jeśli graf Γ' jest izomorficzny z Γ lub z uzupełnieniem grafu Γ, to znaczy z grafem $\langle V, \mathscr{P}_2(V)\setminus E\rangle$. Zadanie nasze polega na znalezieniu liczby klas abstrakcji tak określonej relacji.

Z warunków zadania wynika, że możemy się ograniczyć do rozważania grafów o ustalonym n-elementowym zbiorze wierzchołków V. Każdy graf $\Gamma = \langle V, E\rangle$ możemy przedstawić w postaci funkcji charakterystycznej jego zbioru krawędzi, to znaczy funkcji

$$g\colon \mathscr{P}_2(V) \to \{0, 1\},$$

gdzie $g(\{a, b\}) = 1$ wtedy i tylko wtedy, gdy $\{a, b\} \in E$. Niech G i H oznaczają odpowiednio grupy permutacji zbiorów V i $\{0, 1\}$. Rozszerzymy działanie grupy G na $\mathscr{P}_2(V)$ przyjmując $\alpha\{a, b\} = \{\alpha a, \alpha b\}$, $\alpha \in G$, a, $b \in V$. Dwa grafy o funkcjach charakterystycznych g i g' będą równoważne wtedy i tylko wtedy, gdy istnieją permutacje $\alpha \in G$ i $\beta \in H$ takie, że dla dowolnych $a, b \in A$, $a \neq b$, $\beta g\{a, b\} = g'(\alpha\{a, b\})$.

Oznaczmy przez $G \times H$ iloczyn kartezjański grup G i H, to znaczy grupę złożoną z wszystkich par uporządkowanych $\langle\alpha, \beta\rangle$, $\alpha \in G$, $\beta \in H$, z następującym mnożeniem: $\langle\alpha_1, \beta_1\rangle\ \langle\alpha_2, \beta_2\rangle = \langle\alpha_1\alpha_2, \beta_1\beta_2\rangle$ dla dowolnych $\alpha_1, \alpha_2 \in G$, $\beta_1, \beta_2 \in H$. Zbiór funkcji charakterystycznych grafów ma w naturalny sposób zadaną strukturę prawostronnego G-zbioru i lewostronnego H-zbioru. Zdefiniujmy więc działanie z lewej strony grupy $G \times H$ na tym zbiorze przyjmując, dla $\langle\alpha, \beta\rangle \in G \times H$,

$$\langle\alpha, \beta\rangle g = \beta g \alpha^{-1},$$

gdzie $(\beta g \alpha^{-1})\{a, b\} = \beta(g\{\alpha^{-1}a, \alpha^{-1}b\})$, $\{a, b\} \in \mathscr{P}_2(V)$.

Nasze zadanie polega teraz na odnalezieniu liczby orbit w tym zbiorze przy działaniu grupy $G \times H$.

Jeśli interesowałaby nas po prostu liczba nieizomorficznych grafów, to wystarczyłoby w miejsce grupy H przyjąć grupę, której jedynym elementem jest permutacja identycznościowa.

Innym przykładem sytuacji opisywanej tym samym schematem może być rozkładanie n nierozróżnialnych przedmiotów do m nierozróżnialnych pudełek (niektóre pudełka mogą być puste). Liczba takich rozkładów jest równa liczbie orbit w $S_n \times S_m$-zbiorze wszystkich funkcji ze zbioru $\{1, \ldots, n\}$ w zbiór $\{1, \ldots, m\}$, przy działaniu grupy zdefiniowanym podobnie jak wyżej.

Dalsze warianty, w których rozdzielamy przedmioty na pewne rozróżnialne klasy (n_1 kulek, n_2 sześcianów, n_3 walców, ...), oraz wprowadzamy częściową (lub pełną) rozróżnialność pudełek, pozostawiamy do rozważenia Czytelnikowi.

Niech A będzie dowolnym G-zbiorem. Działanie grupy G na A indukuje w naturalny sposób działanie na A dowolnej podgrupy grupy G, a w szczególności podgrupy cyklicznej (α) generowanej przez operator α należący do G. Zgodnie z

lematem 1.1 A jest sumą rozłączną (α)-orbit. Ze skończoności zbioru A wynika w szczególności, że dla każdego $a \in A$ istnieje najmniejsza liczba naturalna k o tej własności, że $\alpha^k a = \alpha^l a$, gdzie l jest liczbą naturalną mniejszą od k lub zerem, przy czym $\alpha^0 a = a$. Gdyby l było większe od zera, to stosując do obu stron tej równości operator α^{-1} otrzymalibyśmy $\alpha^{k-1} a = \alpha^{l-1} a$ – sprzeczność z założeniem minimalności k. Wobec tego $l = 0$ i (α)-orbita elementu a jest zbiorem $\{\alpha^0 a, \alpha^1 a, \alpha^2 a, \ldots, \alpha^k a\}$. Operator α przestawia cyklicznie elementy tego zbioru po cyklu długości k.

A zatem, dla odróżnienia od orbit będących naszym głównym przedmiotem zainteresowania, (α)-orbity będziemy nazywali *α-cyklami*. W szczególności, dla każdego operatora $\alpha \in G$, zbiór A, na którym działa grupa G, jest sumą rozłączną α-cykli.

Niech $|A| = n$. Dla $i = 1, \ldots, n$ oznaczmy przez $\lambda_i(\alpha)$ liczbę α-cykli długości i. Następujący wielomian n zmiennych $x_1, \ldots, x_n$

$$Z(G, A; x_1, x_2, \ldots, x_n) = |G|^{-1} \sum_{\alpha \in G} x_1^{\lambda_1(\alpha)} x_2^{\lambda_2(\alpha)} \ldots x_n^{\lambda_n(\alpha)}$$

nazywamy *indeksem cyklowym* G-zbioru A. W przypadkach nie budzących wątpliwości będziemy wielomian ten oznaczali przez $Z(G, A)$. Wielomian ten wprowadzili niezależnie Pólya oraz Redfield, który go nazwał *funkcją redukcyjną grupy*.

Zwróćmy uwagę, że jedna i ta sama grupa może działać na zbiorze na wiele istotnie różnych sposobów. Zatem indeks cyklowy powinien być raczej oznaczany poprzez $Z(\sigma)$, gdzie σ jest funkcją opisującą działanie grupy G na zbiorze A. Zachowamy jednak niezbyt poprawne oznaczenie $Z(G, A)$ jako będące bardziej w zgodzie z oznaczeniem powszechnie używanym w literaturze. Zresztą jego użycie nigdy nie będzie prowadziło do nieporozumień.

Dla przykładu pokażemy indeks cyklowy dla rozważanego w poprzednim paragrafie zbioru wierzchołków pięciokąta foremnego, na którym działa grupa D_5 symetrii tego pięciokąta. Łatwo zauważyć, że jest nim następujący wielomian:

$$\tfrac{1}{10}(x_1^5 + 5x_1 x_2^2 + 4x_5).$$

TWIERDZENIE 2.1. *Niech G i H będą grupami działającymi odpowiednio na zbiorach skończonych A i B. Wówczas grupa $G \times H$ działa na zbiorze B^A wszystkich funkcji $f\colon A \to B$ w następujący sposób:*

$$(\langle \alpha, \beta \rangle f)(a) = \beta(f(\alpha^{-1} a)),$$

gdzie $a \in A$, $\langle \alpha, \beta \rangle \in G \times H$, $f \in B^A$.

Liczba orbit grupy $G \times H$ w tym zbiorze jest równa

$$|H|^{-1} \sum_{\beta \in H} Z(G, A; c_1(\beta), c_2(\beta), \ldots, c_{|A|}(\beta)),$$

gdzie $c_i(\beta) = \sum_{s:s|i} s\lambda_s(\beta)$, $i = 1, \ldots, |A|$.

Dowód. Sprawdzenie, że B^A jest $G \times H$-zbiorem pozostawiamy Czytelnikowi. Z Lematu Burnside'a wynika, że poszukiwana liczba orbit jest równa

$$\frac{1}{|G| \cdot |H|} \sum_{\langle\alpha, \beta\rangle \in G \times H} \lambda(\alpha, \beta),$$

gdzie $\lambda(\alpha, \beta)$ oznacza liczbę funkcji $f \in B^A$ takich, że $\langle\alpha, \beta\rangle f = f$.

Rozłóżmy zbiór A na α-cykle i wybierzmy dla każdego α-cyklu reprezentanta. Niech $a \in A$ będzie reprezentantem pewnego α-cyklu długości k i niech $\langle\alpha, \beta\rangle f = f$. Dla każdej liczby całkowitej l mamy $\langle\alpha, \beta\rangle^l f = f$. Wobec tego

$$f(\alpha^l a) = (\langle\alpha, \beta\rangle^l f)(\alpha^l a) = \beta^l f \alpha^{-l} \alpha^l a = \beta^l (fa).$$

W szczególności

$$fa = f(\alpha^k a) = \beta^k (fa).$$

A zatem obraz reprezentanta a musi być punktem stałym operatora β^k. Na odwrót, wybierając dowolny punkt stały b operatora β^k możemy zdefiniować funkcję określoną na cyklu $(\alpha)a$ przyjmując

$$f(\alpha^l a) = \beta^l b, \qquad l \text{ całkowite.}$$

Wtedy $(\langle\alpha, \beta\rangle f)(\alpha^l a) = \beta f(\alpha^{l-1} a) = \beta\beta^{l-1} b = f(\alpha^l a)$. Skoro A jest sumą rozłączną α-cykli, to definiując w powyższy sposób funkcję $f \in B^A$ na każdym cyklu z osobna otrzymamy funkcję o własności $\langle\alpha, \beta\rangle f = f$.

Wynika stąd, że $\lambda(\alpha, \beta)$ jest równe liczbie możliwości wyboru punktów stałych odpowiednich potęg operatora β. Jeżeli a jest reprezentantem cyklu długości k, to jego obraz $b \in B$ może być dowolnym z s elementów pewnego β-cyklu długości s, gdzie s jest dzielnikiem k. Wobec tego obraz a można wybrać na $\sum_{s:s|k} s\lambda_s(\beta)$ sposobów, a więc

$$\lambda(\alpha, \beta) = \prod_{i=1}^{n} \sum_{s:s|i} s\lambda_s(\beta)^{\lambda_i(\alpha)}.$$

Zatem szukana liczba orbit jest równa

$$\frac{1}{|H|} \sum_{\beta \in H} \frac{1}{|G|} \sum_{\alpha \in G} \lambda(\alpha, \beta) = \frac{1}{|H|} \sum_{\beta \in H} \frac{1}{|G|} \sum_{\alpha \in G} \prod_{i=1}^{n} \Big(\sum_{s:s|i} s\lambda_s(\beta)^{\lambda_i(\alpha)}\Big),$$

co jest żądanym wynikiem.

Wniosek 2.2 (Pólya [1]). *Niech będzie dane lewostronne działanie grupy G na skończonym zbiorze A oraz m-elementowy zbiór B. Przyjmując $(f\alpha)a = f(\alpha a)$ dla wszystkich $f \in B^A$, $\alpha \in G$ i $a \in A$, określamy na zbiorze funkcji B^A prawostronne działanie grupy G, dla którego liczba orbit w zbiorze B^A jest równa*

$$Z(G, A; m, m, \ldots, m) = |G|^{-1} \sum_{\alpha \in G} m^{c(\alpha)},$$

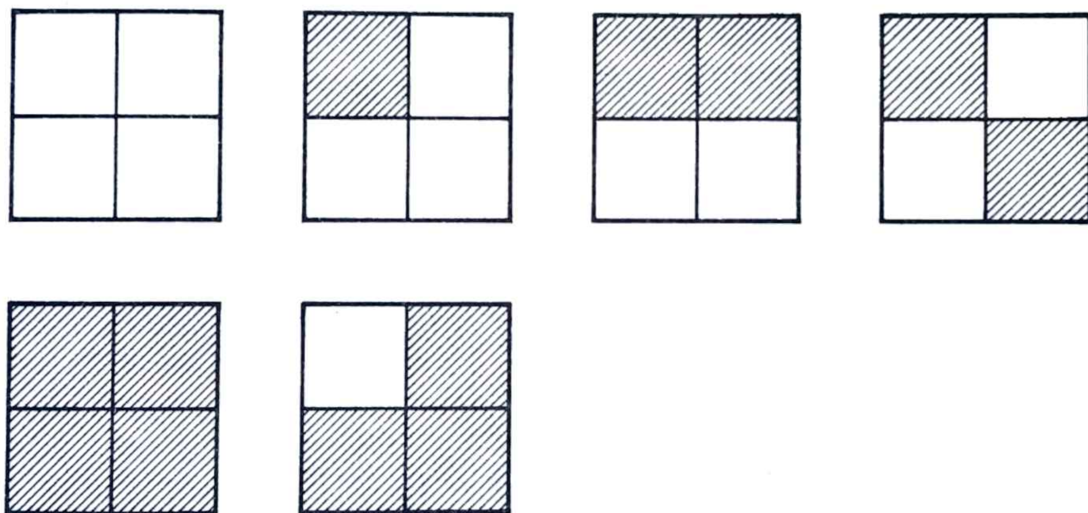
gdzie $c(\alpha)$ oznacza liczbę α-cykli w rozkładzie G-zbioru A.

Dowód. Na zbiorze B działa grupa E złożona wyłącznie z elementu neutralnego. Należy teraz jedynie zauważyć, że orbity na zbiorze B^A przy działaniu grupy $G \times E$ z lewej i grupy G z prawej są takie same, i zastosować poprzednie twierdzenie. □

Powróćmy do problemu malowania czteropolowej szachownicy rozważanego w paragrafie 1. Załóżmy, że pola wyznaczone są na kwadratowej desce. Wtedy zbiorem A będzie zbiór tych pól, i działa na nim jako grupa obrotów czteroelementowa cykliczna grupa C_4. Łatwo sprawdzić, że

$$Z(C_4, A) = \tfrac{1}{4}(x_1^4 + x_2^2 + 2x_4).$$

Wobec tego szachownicę można pomalować dwoma kolorami na $\frac{1}{4}(2^4+2^2+ +2^2) = 2^2+1+1 = 6$ sposobów.



Rys. 27. Wszystkie istotnie różne sposoby pokolorowania szachownicy wymiaru 2×2

Wszystkie te sposoby pokazano na rys. 27. Jeżeli istotne jest tylko, by kolory były różne, tzn. jeśli są one wzajemnie zamienialne, to na zbiorze kolorów działa grupa C_2, której elementy oznaczymy przez 1 i β. Mamy $c_1(1) = c_2(1) = c_4(1) = = c_2(\beta) = c_4(\beta) = 2$ i $c_1(\beta) = 0$. Wobec tego istnieją

$$\tfrac{1}{2}\big(\tfrac{1}{4}(2^4+2^2+2\cdot 2)+\tfrac{1}{4}(2^2+2\cdot 2)\big) = \tfrac{1}{2}(6+2) = 4$$

istotnie różne sposoby pomalowania, co także ilustruje rysunek 27. Czytelnik zechce sprawdzić, że analogiczne zadania dla kwadratowej szachownicy o dziewięciu polach dadzą odpowiednio 140 i 70 sposobów pomalowania, czego już ilustrować nie będziemy (jak wyglądają odpowiedzi, gdy na polach szachownicy działają inne grupy wymienione w paragrafie 1?).

Innego przykładu mogą dostarczyć pokolorowania sześcianu nie przechodzące na siebie przy obrotach sześcianu w przestrzeni trójwymiarowej.

Położenie sześcianu jest w tym przypadku wyznaczone jednoznacznie przez

położenie dwóch sąsiadujących ze sobą wierzchołków. Łatwo zauważyć, że ustalony wierzchołek można sprowadzić za pomocą obrotów do dowolnej spośród ośmiu pozycji. Jego sąsiad w każdym z tych przypadków może zająć trzy różne położenia. Wobec tego grupa obrotów sześcianu ma 24 elementy. Odszukajmy cykle elementów tej grupy działającej na zbiorze ścian sześcianu. Poza przekształceniem identycznościowym, które ma sześć cykli długości 1, mamy w tej grupie trzy razy po trzy obroty wokół osi przechodzących przez środki przeciwległych ścian. Każdy z tych obrotów ma dwa cykle długości jeden i albo cykl długości cztery — w sześciu przypadkach, albo dwa cykle długości dwa — w trzech przypadkach. Następnie jest sześć klas obrotów nieidentycznościowych wokół osi przechodzących przez środki przeciwległych krawędzi — każda składa się z jednego obrotu o trzech cyklach długości dwa. Na koniec cztery klasy obrotów wokół osi przechodzących przez przeciwległe wierzchołki — w każdej po dwa obroty o dwóch cyklach długości trzy. Wobec tego szukany indeks cyklowy jest następującym wielomianem

$$\tfrac{1}{24}(x_1^6+6x_1^2x_4+3x_1^2x_2^2+6x_2^3+8x_3^2).$$

Fakt, że suma współczynników wielomianu jest równa 1 gwarantuje nam, że przy obliczaniu indeksu cyklowego żaden operator z grupy nie został pominięty. Wobec powyższego, malując ściany sześcianu na, powiedzmy, dwa kolory uzyskamy

$$\tfrac{1}{24}(2^6+6\cdot 2^2\cdot 2+3\cdot 2^2\cdot 2^2+6\cdot 2^8+8\cdot 2^2)=10$$

różnych sposobów pomalowania.

Odnotujmy, że ponieważ środki ścian sześcianu są wierzchołkami ośmiościanu foremnego, to indeks cyklowy zbioru wierzchołków ośmiościanu z działającą na nim grupą obrotów jest tym samym wielomianem, co policzony powyżej.

Podobnie, te same indeksy cyklowe otrzymamy dla zbiorów wierzchołków sześcianu i ścian ośmiościanu, na których działa ta sama grupa.

Rozważmy wreszcie S_m-zbiór B^A wszystkich funkcji z n-elementowego zbioru A w $B=\{1, \ldots, m\}$. (S_m oznacza, jak zwykle, grupę permutacji zbioru B i permutacje działają na funkcjach z B^A poprzez złożenia.) Orbita funkcji f składa się ze wszystkich takich funkcji, dla których podział zbioru A na przeciwobrazy elementów zbioru B jest taki sam jak dla f. Wobec tego liczba S_m-orbit w B^A jest równa liczbie podziałów zbioru A na co najwyżej m podzbiorów. Indeks cyklowy E-zbioru A, gdzie E jest grupą identycznościową, jest równy x_1^n. Zatem, zgodnie z twierdzeniem 1, szukana liczba orbit jest równa

$$\frac{1}{m!}\sum_{\beta\in S_m}(\lambda_1(\beta))^n.$$

Jeżeli przez D_l oznaczymy liczbę permutacji zbioru o l elementach nie mających punktów stałych, to permutacji zbioru m-elementowego mających dokładnie k

punktów stałych jest $\binom{m}{k}D_{m-k}$. Wobec tego powyższa suma jest równa

$$\frac{1}{m!}\sum_{k=0}^{m}\binom{m}{k}D_{m-k}k^n.$$

Po skorzystaniu ze wzoru

$$D_l = l!\sum_{j=0}^{l}\frac{(-1)^j}{j!}$$

(por. rozdział 1, twierdzenie 7.4), podstawieniu i uproszczeniach otrzymujemy, że podziałów zbioru n-elementowego na co najwyżej m części jest

$$\sum_{k=0}^{m}\frac{k^n}{k!}\sum_{j=0}^{m-k}\frac{(-1)^j}{j!}.$$

W szczególności, jeżeli $m \geqslant n$, to otrzymana liczba jest liczbą wszystkich podziałów zbioru n-elementowego, czyli liczbą Bella B_n (por. rozdział 1, § 8).

§ 3. Wyznaczanie indeksów cyklowych

Niech G będzie grupą, zaś A zbiorem. Działanie grupy G na zbiorze A określa homomorfizm grupy G w grupę S_A permutacji zbioru A. Elementowi α homomorfizm ten przypisuje permutację f_α taką, że $f_\alpha(a) = \alpha a$, dla każdego $a \in A$. Prawdziwa jest też zależność odwrotna. Każdy homomorfizm grupy G w grupę S_A zadaje nam, w naturalny sposób, działanie grupy G na A. Jeżeli homomorfizm ten jest przekształceniem różnowartościowym, to mówimy, że działanie grupy G na A jest *wierne*.

Działanie G na A oczywiście nie musi być wierne, jednakże orbity A będą takie same zarówno dla grupy G jak i dla jej obrazu $\hat{G}$ w grupie S_A. Wobec tego indeksy cyklowe dla G-zbioru A i $\hat{G}$-zbioru A muszą być takie same. Różnica jest jedynie taka, że przy obliczaniu indeksu cyklowego odpowiadającego grupie G pomnożymy mianownik oraz współczynnik przy każdym jednomianie przez liczbę elementów przechodzących przy wspomnianym homomorfizmie na jedynkę grupy G.

Z powyższych uwag wynika, że w praktycznych obliczeniach wygodniej obliczać indeksy cyklowe dla grup działających wiernie lub, co na to samo wychodzi, dla podgrup grup permutacji. Ogólna definicja G-zbioru została wprowadzona z tej przyczyny, że jest ona znacznie wygodniejsza w dowodach twierdzeń. W związku z tym, jeżeli wiadomo na jakim zbiorze działa grupa permutacji, to w ogólnie przyjętej notacji indeksu cyklowego zbioru tego się nie zaznacza. Tak więc $Z(S_n)$ oznacza, w poprzednim zapisie, $Z(S_n, \{1, \ldots, n\})$.

Ponadto używa się specjalnych oznaczeń dla obrazów izomorficznych grupy

będących podgrupami grup permutacji innych zbiorów. Tak więc, dla przykładu, $S_n^{(k)}$ i $S_n^{[k]}$ oznaczają odpowiednie obrazy grupy S_n działającej na zbiorach $\mathscr{P}_k(A)$ i A^k, gdzie $A = \{1, \ldots, n\}$, operator zaś $\alpha \in S_n$ odwzorowuje k-elementowy podzbiór zbioru A na zbiór złożony z obrazów elementów. Podobnie działa operator α na ciągach długości k.

W ten sam sposób, przez E_n oznacza się grupę, której jedynym elementem jest przekształcenie identycznościowe na $\{1, \ldots, n\}$. Będziemy także używali tej i podobnych konwencji w przypadkach nie prowadzących do nieporozumień.

Stosując tę notację mamy oczywiście

$$Z(E_n) = x_1^n.$$

Rozważmy teraz grupę S_n. Każdą permutację zbioru $\{1, \ldots, n\}$ można przedstawić, jak wiadomo, w postaci iloczynu rozłącznych permutacji cyklicznych. Z twierdzenia Cauchy'ego (twierdzenie 1.4.2) permutacji typu $d = 1^{d_1} 2^{d_2} \ldots n^{d_n}$ jest

$$\frac{n!}{1^{d_1} d_1! 2^{d_2} d_2! \ldots n^{d_n} n!}.$$

Wobec tego

$$Z(S_n) = \sum_d \prod_{i=1}^{n} \frac{1}{d_i!} \left(\frac{x_i}{i}\right)^{d_i},$$

gdzie sumowanie przebiega po wszystkich rozwiązaniach w nieujemnych liczbach całkowitych równania $1d_1 + 2d_2 + \ldots + nd_n = n$.

Podobnie łatwo obliczyć, że dla grupy alternującej A_n składającej się ze wszystkich permutacji zbioru $\{1, \ldots, n\}$, które mają parzystą liczbę cykli długości parzystej, mamy

$$Z(A_n) = \sum_d \left(1 + (-1)^{d_2 + d_4 + \ldots}\right) \prod_{i=1}^{n} \frac{1}{d_i!} \left(\frac{x_i}{i}\right)^{d_i} =$$
$$= Z(S_n; x_1, x_2, x_3, x_4, \ldots) + Z(S_n; x_1, -x_2, x_3, -x_4, \ldots).$$

Rozpatrzmy teraz wszystkie permutacje, w których element n występuje w cyklu długości i, $i = 1, \ldots, n$. Pozostałe elementy cyklu można wybrać na $\binom{n-1}{i-1}$ sposobów i ustawić je w danym cyklu na $(i-1)!$ sposobów. Rozkład pozostałych cykli w rozważanej permutacji dany jest wielomianem $(n-i)!\, Z(S_{n-i})$, gdzie $Z(S_0) = 1$. Wobec tego

$$Z(S_n) = \frac{1}{n!} \sum_{i=1}^{n} (n-1)!\, Z(S_{n-1}) \binom{n-1}{i-1} (i-1)!\, x_i =$$
$$= \frac{1}{n} \sum_{i=1}^{n} Z(S_{n-1}) x_i,$$

co daje wzór rekurencyjny na indeks $Z(S_n)$.

Rozumując w sposób podobny do przedstawionego powyżej można łatwo stwierdzić, że dla grupy D_n symetrii n-kąta foremnego działającej na zbiorze jego wierzchołków (albo na zbiorze boków) mamy

$$Z(D_n) = \tfrac{1}{2}Z(C_n) + \begin{cases} \tfrac{1}{2}x_1 x_2^{(n-1)/2}, & \text{jeżeli } n \text{ nieparzyste,} \\ \tfrac{1}{4}(x_2^{n/2} + x_1^2 x_2^{(n-2)/2}), & \text{jeżeli } n \text{ parzyste.} \end{cases}$$

C_n oznacza tu n-elementową grupę cykliczną. Wybierając jako tę grupę addytywną grupę reszt modulo n, za pomocą bezpośrednich rachunków łatwo otrzymujemy

$$Z(C_n) = \frac{1}{n} \sum_{i:i|n} \varphi(i) x_i^{n/i},$$

gdzie φ jest funkcją Eulera (por. rozdział 2, § 5). Jest to szczególny przypadek sytuacji, w której grupa G działa na zbiorze swoich elementów mnożąc je z lewej strony. Oznaczając przez $\varrho(i)$ liczbę elementów rzędu i w G mamy

(3.1) $$Z(G) = \frac{1}{|G|} \sum_{i:i||G|} \varrho(i) x_i^{|G|/i}.$$

Podkreślmy tu jeszcze raz, że w istocie indeks cyklowy zależy od działania grupy, a nie tylko od samej grupy, nawet wtedy, gdy działa ona wiernie. Stosując powyższy wzór do grupy S_n, a więc do grupy S_n działającej wiernie poprzez składanie permutacji na zbiorze S_n, otrzymamy zupełnie inny indeks cyklowy $Z(S_n)$ niż uprzednio policzony indeks $Z(S_n)$. Ten pierwszy odnosił się do wiernego działania grupy S_n jako grupy permutacji zbioru $\{1, \ldots, n\}$. Nawet ta sama grupa działająca na tym samym zbiorze, i to wiernie, może w różnych przypadkach mieć różne indeksy cyklowe. Przykładu może tu dostarczyć grupa C_2 działająca na zbiorze $\{1, 2, 3, 4\}$. Za pierwszym razem element rzędu 2 przestawia między sobą liczby 1 i 2, zaś 3 i 4 są jego punktami stałymi. Za drugim tenże sam element zamieni parami 1 z 2 i 3 z 4. Czytelnik zechce sprawdzić, że indeksy cyklowe są rzeczywiście różne. Wynika z tego, że we wszystkich wątpliwych przypadkach należy jasno określić działanie grupy, do którego dany indeks się odnosi.

Odnotujmy ponadto fakt, że z równości cyklowych indeksów wcale nie musi wynikać istnienie izomorfizmu odpowiednich grup – nawet działających wiernie. Tym bardziej nie muszą być izomorficzne odpowiednie G-zbiory (definicję izomorfizmu G-zbiorów pozostawiamy do sformułowania Czytelnikowi). Na przykład, wiadomo z teorii grup, że istnieje nieabelowa grupa G rzędu 3^3, w której każdy element, różny od neutralnego, ma rząd 3. Jako grupę H przyjmijmy grupę abelową $C_3 \times C_3 \times C_3$. Grupy te będą działały każda na sobie przez mnożenie. Ze wzoru (3.1) mamy

$$Z(G) = Z(H),$$

lecz grupy G i H oczywiście nie są izomorficzne.

Ważne zastosowania kombinatoryczne mają indeksy cyklowe $Z(S_n^{(2)})$ i $Z(S_n^{[2]})$ używane przy zliczaniu odpowiednio grafów i grafów zorientowanych. Powtarzając

w zasadzie rozumowanie pokazane przy okazji obliczania liczby turniejów, łatwo jest stwierdzić, iż pary o elementach należących do jednego α-cyklu dlugości $2i+1$ dadzą i cykli, każdy długości $2i+1$. Wobec tego czynnik x_{2i+1}, $1 \leqslant 2i+1 \leqslant n$, z indeksu $Z(S_n)$ da nam czynnik x_{2i+1}^i w $Z(S_n^{(2)})$. Podobnie x_{2i}, $1 \leqslant 2i \leqslant n$, przejdzie na czynnik $x_i x_{2i}^{i-1}$. Uwzględniając natomiast pary o elementach z dwóch różnych α-cykli o długościach odpowiednio i oraz j uzyskamy z czynnika $x_i s_j$ czynnik $x_{[i,j]}^{(i,j)}$. Wobec tego

$$Z(S_p^{(2)}) = \sum_d \frac{1}{\prod\limits_{k=1}^{n} d_k!\,k^{d_k}} \prod_{i=0}^{\lfloor n/2-1 \rfloor} x_{2i+1}^{id_{2i+1}} \prod_{i=1}^{\lfloor n/2 \rfloor} (x_i x_{2i}^{i-1})^{d_i} \times$$

$$\times \prod_{i=1}^{n} x_i^{i\binom{d_i}{2}} \prod_{i,j:1 \leqslant i<j \leqslant n} x_{[i,j]}^{(i,j)} d_i d_j.$$

Podobnie

$$Z(S_p^{[2]}) = \sum_d \frac{1}{\prod\limits_{k=1}^{n} d_k!\,k^{d_k}} \prod_{i=1}^{n} x_i^{(i-1)d_i + 2i\binom{d_i}{2}} \prod_{i,j:1 \leqslant i<j \leqslant n} x_{[i,j]}^{2(i,j)d_i d_j},$$

gdzie sumowanie przebiega po wszystkich $d = \langle d_1, \ldots, d_n \rangle$ takich, że

$$1d_1 + 2d_2 + \ldots + nd_n = n, \qquad d_1, \ldots, d_n \geqslant 0.$$

Tablicę wielomianów $Z(S_n)$ i $Z(S_n^{[2]})$ dla $n \leqslant 10$ można znaleźć w książce Harary'ego i Palmera [1].

Powróćmy do rozważanego na początku paragrafu 2 przykładu grafów nierównoważnych o n wierzchołkach.

Jeżeli $n=3$, to $Z(S_3^{(2)}) = Z(S_3)$, ponieważ istnieje wzajemnie jednoznaczna odpowiedniość pomiędzy parami a zbiorami jednoelementowymi, które są ich uzupełnieniami. Wobec tego szczegółowe rachunki pozostawiamy Czytelnikowi.

Rozważmy przypadek $n=4$. Korzystając z podanego wzoru otrzymujemy

$$Z(S_4^{(2)}) = \tfrac{1}{24}(x_1^6 + 9x_1^2 x_2^2 + 8x_3^2 + 6x_2 x_4).$$

Stosujemy teraz twierdzenie 2.1.Oznaczając elementy grupy S_2 przez 1 i β mamy

$$c_1(1) = c_2(1) = c_3(1) = c_4(1) = 2,$$
$$c_1(\beta) = c_3(\beta) = 0,$$
$$c_2(\beta) = c_4(\beta) = 2.$$

Wobec tego szukana liczba jest równa

$$\tfrac{1}{48}(2^6 + 9\cdot 2^2 \cdot 2^2 + 8\cdot 2^2 + 6\cdot 2\cdot 2 + 6\cdot 2\cdot 2) = \tfrac{16}{48}(2^2 + 9 + 2 + 3) = \tfrac{1}{3}\cdot 18 = 6.$$

Mnożąc tę liczbę przez 2 otrzymamy liczbę grafów o czterech wierzchołkach, przy

czym każdy graf izomorficzny ze swoim uzupełnieniem został policzony dwukrotnie. Ponieważ grafów czterowierzchołkowych jest $Z(S_4^{(2)}; 2, 2, 2, 2) = 11$, więc istnieje (z dokładnością do izomorfizmu) dokładnie jeden samouzupełnialny graf o czterech wierzchołkach (jaki?). Uwagę tę można uogólnić (por. zad. 4).

Na zakończenie tego paragrafu odnotujemy jeszcze dwie proste własności indeksu cyklowego, które pozwalają czasami na uproszczenie obliczeń.

TWIERDZENIE 3.1. *Niech $A = \{a_{ij}: 1 \leqslant i \leqslant n \wedge 1 \leqslant j \leqslant m\}$. Załóżmy, że grupa G działa na zbiorze A w taki sposób, że dla każdego $\alpha \in G$ i dla każdego $j \in \{1, \ldots, m\}$ istnieje $k \in \{1, \ldots, m\}$ takie, że dla każdego $i \in \{1, \ldots, n\}$*

$$\alpha a_{ij} = a_{ik}.$$

Jeżeli

$$A_1 = \{a_{11}, a_{12}, \ldots, a_{1m}\},$$

to

$$Z(G, A; x_1, x_2, \ldots, x_{mn}) = Z(G, A_1; x_1^n, x_2^n, \ldots, x_m^n).$$

Dowód. α-cykl elementu a_{ij} składa się dokładnie z tych elementów a_{ik}, dla których a_{1k} należy do α-cyklu elementu a_{1j}. Wobec tego każdy α-cykl w A_1 daje n α-cykli tej samej długości w A i wszystkie cykle w A powstają w ten sposób. Teza wynika z definicji $Z(G, A)$. □

Niech grupy G i H działają na rozłącznych zbiorach A i B. Zdefiniujemy działanie grupy $G \times H$ na sumie $A \cup B$ przyjmując dla $\langle \alpha, \beta \rangle \in G \times H$,

$$\langle \alpha, \beta \rangle a = \begin{cases} \alpha a, & \text{jeżeli } a \in A, \\ \beta a, & \text{jeżeli } a \in B. \end{cases}$$

Obraz grupy $G \times H$ w grupie permutacji zbioru $A \cup B$ oznaczymy przez $G \dot{\cup} H$.

TWIERDZENIE 3.2. *Dla określonego powyżej działania grupy $G \times H$ mamy*

$$Z(G \dot{\cup} H) = Z(G) \cdot Z(H).$$

Dowód. Niech

$$Z(G, A) = \frac{1}{|G|} \sum_{\alpha \in G} x_1^{\lambda_1(\alpha)} \ldots x_n^{\lambda_n(\alpha)},$$

$$Z(H, B) = \frac{1}{|H|} \sum_{\beta \in H} y_1^{\lambda_1(\beta)} \ldots y_m^{\lambda_m(\beta)}.$$

Jeżeli $\langle \alpha, \beta \rangle \in G \times H$, to operator ten działa na elementach z A jak α, a na elementach z B jak β. Wobec tego rozkład długości $\langle \alpha, \beta \rangle$-cykli jest opisany jednomianem

$$w(\alpha, \beta) = x_1^{\lambda_1(\alpha)} x_2^{\lambda_2(\alpha)} \ldots x_n^{\lambda_n(\alpha)} y_1^{\lambda_1(\beta)} y_2^{\lambda_2(\beta)} \ldots y_m^{\lambda_m(\beta)},$$

zatem

$$Z(G \dot{\cup} H) = \frac{1}{|G|\cdot|H|} \sum_{\langle\alpha,\beta\rangle\in G\times H} w(\alpha, \beta) = Z(G)\cdot Z(H). \quad \square$$

Z powyższych twierdzeń skorzystamy dla znalezienia indeksu cyklowego zbioru pól szachownicy kwadratowej, na której działa czteroelementowa grupa G obrotów kwadratu.

Zacznijmy od szachownicy o boku $2n$. $4n^2$ pól tej szachownicy można podzielić na n^2 czteroelementowych zbiorów $A_1, A_2, \ldots, A_{n^2}$, których elementy są ponumerowane w taki sposób, że są spełnione założenia twierdzenia 3.1 (por. rys. 28 dla $n = 2$).

11	21	31	12
34	41	42	22
24	44	43	32
14	33	23	13

Rys. 28. Numeracja zgodna z twierdzeniem 3.1. Druga liczba numeruje kolejno elementy orbity o numerze danym przez pierwszą liczbę

Grupa G działa na zbiorze $\{A_k\colon 1 \leqslant k \leqslant n^2\}$ jak na polach szachownicy 2×2. Indeksem cyklowym dla tej ostatniej jest wielomian $\frac{1}{4}(x_1^4 + x_2^2 + 2x_4)$ (zob. (2.1)). Wobec twierdzenia 3.1, poszukiwanym indeksem jest wielomian $\frac{1}{4}(x_1^{4n^2} + x_2^{2n^2} + 2x_4^{n^2})$.

Jeżeli teraz szachownica ma bok długości $2n+1$, to działanie grupy obrotów G możemy zastąpić działaniem grupy $G \dot{\cup} E$, gdzie E działa na polu środkowym, a grupa G na $4n(n+1)$ pozostałych polach. Wobec powyższego, korzystając z twierdzenia 3.2 otrzymujemy, że poszukiwany indeks ma postać

$$\tfrac{1}{4}x_1\,(x_1^{4n(n+1)} + x_2^{2n(n+1)} + 2x_4^{n(n+1)}).$$

Rozważmy jeszcze zadanie polegające na znalezieniu liczby sposobów umieszczenia dwóch identycznych kulek i trzech sześcianów w dwóch rozróżnialnych pudełkach. Zadanie jest równoważne pytaniu o liczbę funkcji w zbiór $\{0, 1\}$ z pięcioelementowego zbioru, na którym działa grupa $S_2 \dot{\cup} S_3$. Indeksem cyklowym jest wobec tego

$$\frac{1}{2!\,3!}(x_1^2 + x_2)(x_1^3 + 3x_1x_2 + 2x_3)$$

i mamy $\dfrac{1}{2\cdot 6}(4+2)(8+12+4) = 12$ sposobów rozmieszczenia.

§ 4. Zliczanie orbit funkcji za pomocą wag

Rozwinięte w tym rozdziale metody pozwalają, w gruncie rzeczy, na wyznaczenie nie tylko liczby orbit w zbiorze funkcji z danego G-zbioru w pewien H-zbiór, ale także na uzyskanie znacznie głębszych informacji. Można mianowicie znaleźć liczbę orbit, których reprezentantami są funkcje o przeciwobrazach zadanej z góry liczności. Powracając do otwierającego rozdział przykładu naszyjników o pięciu paciorkach możemy policzyć, że np. są dwa naszyjniki o trzech paciorkach białych i dwóch czarnych. Do tego celu potrzebna nam będzie metoda pozwalająca na wyróżnianie orbit w zbiorze funkcji. Dostarczają jej tak zwane wagi.

Niech R będzie dowolnym pierścieniem przemiennym zawierającym jako podpierścień ciało liczb wymiernych Q (jedynka ciała Q jest jedynką w R). Niech M będzie jego dowolnym multyplikatywnie zamkniętym podzbiorem o tej własności, że dowolny element $m \in M$ można przedstawić jedynie na skończenie wiele sposobów w postaci $m = m_1 \cdot m_2$, gdzie $m_1, m_2 \in M$. Przykładem najczęściej spotykanym w zastosowaniach będzie pierścień $R = Q[y]$ wielomianów jednej zmiennej y, gdzie $M = \{1, y, y^2, \ldots\}$.

M-szeregiem formalnym — lub, w skrócie, szeregiem — będziemy nazywali dowolną funkcję $\varphi: M \to Q$. Sumę szeregów φ i ψ definiujemy jako szereg $\varphi + \psi$, dla którego

$$(\varphi+\psi)(m) = \varphi(m)+\psi(m).$$

Ich iloczynem jest szereg $\varphi \cdot \psi$, gdzie

$$(\varphi \cdot \psi)(m) = \sum \{\varphi(m_1) \cdot \psi(m_2): \ m_1 \cdot m_2 = m \wedge m_1, m_2 \in M\}.$$

Łatwo jest sprawdzić, że M-szeregi formalne tworzą pierścień przemienny. Szereg φ będziemy zapisywali w postaci

$$\varphi = \sum_{m \in M} \varphi(m)m.$$

Elementy tak zdefiniowanego pierścienia dodaje się i mnoży tak jak zwykłe wielomiany. Powyższa definicja jest nieco zmienioną i rozszerzoną wersją definicji szeregów formalnych z rozdziału 3 i łatwo dostrzec, że się od niej istotnie nie różni.

Niech B będzie zbiorem — niekoniecznie skończonym — na którym działa skończona grupa H. *Wagą względem działania grupy H* będziemy nazywali każdą funkcję $w: B \to M$, która jest stała na orbitach grupy H i taką, że zbiór $w^{-1}(m)$ jest skończony dla każdego $m \in M$. Element $w(b)$, $b \in B$, będziemy nazywali *wagą elementu b*. Wobec powyższej definicji jest tylko skończenie wiele elementów z B o tej samej wadze*.

Przypuśćmy teraz, że jest dany zbiór skończony A, na którym działa grupa skończona G.

---

* Słowo „waga" jest tu używane w dwóch znaczeniach, jak w wyrażeniach „funkcja sinus" i „sinus 30°". Jest to nie całkiem poprawne, lecz wygodne.

Przypomnijmy, że zbiór funkcji B^A jest $G\times H$-zbiorem, gdzie $\langle\alpha, \beta\rangle f = \beta f\alpha^{-1}$ dla $f\in B^A$, $\langle\alpha, \beta\rangle\in G\times H$. Zdefiniujmy funkcję

$$w^*\colon\ B^A \to M$$

przyjmując $w^*(f) = \prod_{a\in A} w(f(a))$, $f\in B^A$.

LEMAT 4.1. *Funkcja* $w^*\colon B^A\to M$ *jest wagą względem działania grupy* $G\times H$.

Dowód.

$$w^*(\langle\alpha, \beta\rangle f) = \prod_{a\in A} w(\beta f(\alpha^{-1}a)) = \prod_{a\in A} w(\beta f(a)) = \prod_{a\in A} w(f(a)) = w^*(f).$$

Przedostatnia równość wynika z tego, że funkcja w jest stała na H-orbitach. Zatem funkcja w^* jest stała na $G\times H$-orbitach. Skończoność przeciwobrazów funkcji w^* wynika z własności zbioru M i skończoności zbioru A. Ustalmy wagę $w\colon B\to M$, a więc i wagę $w^*\colon B^A\to M$. *Wagą orbity* nazwiemy wagę jej dowolnego elementu. Oznaczmy przez o_m liczbę $G\times H$-orbit wagi $m\in M$ w zbiorze B^A i niech

$$\Omega = \sum_{m\in M} o_m m.$$

Oznaczmy ponadto przez $\lambda_s^m(\beta)$ liczbę β-cykli długości s i wagi m w zbiorze B.

TWIERDZENIE 4.2 (de Bruijn [1]). *Niech G i H będą grupami skończonymi działającymi odpowiednio na zbiorze skończonym A i na zbiorze B i niech grupa $G\times H$ działa na zbiorze B^A w następujący sposób: $\langle\alpha, \beta\rangle f = \beta f\alpha^{-1}$ dla $f\in B^A$, $\langle\alpha, \beta\rangle\in G\times H$. Wówczas*

$$\Omega = |H|^{-1}\sum_{\beta\in H} Z(G, A;\, c_1(\beta), c_2(\beta), \ldots, c_{|A|}(\beta)),$$

gdzie $c_i(\beta)$ jest szeregiem

$$\sum_{m\in M}\sum_{s:s|i} s\lambda_s^m(\beta) m^i.$$

Dowód. Rozważmy podzbiór zbioru B^A składający się z funkcji wagi m. Funkcja w^* jest wagą, zatem zbiór ten jest $G\times H$-zbiorem z działaniem indukowanym przez działanie grupy $G\times H$ na całym zbiorze B^A. Z lematu Burnside'a wynika wobec tego, że

$$o_m = \frac{1}{|G|\cdot|H|}\sum_{\langle\alpha,\beta\rangle\in G\times H}\lambda^m(\alpha, \beta),$$

gdzie $\lambda^m(\alpha, \beta)$ oznacza liczbę funkcji f wagi m takich, że $\langle\alpha, \beta\rangle f = f$. Jeżeli szereg $\sum_{m\in M}\lambda^m(\alpha, \beta)m$ oznaczymy przez $\lambda(\alpha, \beta)$, to wobec powyższego mamy

(4.1) $$\Omega = \sum_{m\in M} o_m m = \frac{1}{|G|\cdot|H|}\sum_{\langle\alpha,\beta\rangle\in G\times H}\lambda(\alpha, \beta).$$

Niech $f \in B^A$ będzie funkcją taką, że $\langle\alpha, \beta\rangle f = f$, i niech $a \in A$ należy do α-cyklu długości k. Podobnie jak w dowodzie twierdzenia 2.1 wykazujemy, że f można zdefiniować na cyklu $(\alpha)a$ na dokładnie tyle sposobów, ile istnieje elementów $b \in B$ takich, że $\beta^k b = b$. Zauważmy ponadto, że $f(\alpha^l a) = \beta^l(fa) = \beta^l b$, a więc obraz α-cyklu $(\alpha)a$ jest zawarty w β-cyklu $(\beta)b$. Wobec powyższego przy obliczaniu $w^*(f)$ cykl $(\alpha)a$ daje nam czynnik $w(b)^k$, gdzie $b = fa$.

Jak wiemy, α-cykle są rozłączne i ich suma pokrywa cały zbiór A. Zatem przy definiowaniu punktów stałych operatora $\langle\alpha, \beta\rangle$ możemy wybierać odpowiednie obrazy, a więc i ich wagi, niezależnie. Wobec tego

$$\lambda(\alpha, \beta) = \prod_{i=1}^{n} \Big(\sum_{b:b=\beta^i b} w(b)^i \Big)^{\lambda_i(\alpha)}.$$

Porządkując każdy czynnik iloczynu według wag i powtarzając, dla każdej wagi $m \in M$, odpowiedni fragment dowodu twierdzenia 2.1 otrzymujemy

$$\sum_{b:b=\beta^i b} w(b)^i = \sum_{m\in M} \Big(\sum_{s:s|i} s\lambda_s^m(\beta)\Big) m^i,$$

gdzie $\lambda_s^m(\beta)$ jest liczbą β-cykli długości s w zbiorze $w^{-1}(m)$.

Podstawiając teraz obliczony szereg $\lambda(\alpha, \beta)$ do znalezionego wzoru (4.1) na Ω kończymy dowód twierdzenia. □

Wniosek 4.3 (Pólya [1]). *Niech będzie dane działanie lewostronne grupy G na zbiorze skończonym A i niech funkcja $w\colon B \to M$ będzie wagą na pewnym zbiorze B. Przyjmując $(f\alpha)a = f(\alpha a)$ dla wszystkich $f \in B^A$, $\alpha \in G$ i $a \in A$, określamy na zbiorze funkcji B^A działanie prawostronne grupy G, dla którego*

$$\Omega = \sum_{m\in M} o_m m = Z\big(G, A; c(m), c(m^2), c(m^3), \ldots\big),$$

gdzie o_m jest liczbą G-orbit wagi m w zbiorze B^A, a $c(m) = \sum_{m\in M} |w^{-1}(m)| m$.

Dowód. Wystarczy zastosować poprzednie twierdzenie w przypadku, gdy $H = E = \{\varepsilon\}$. Wówczas

$$c_i(\varepsilon) = \sum_{m\in M} \Big(\sum_{s:s|i} s\lambda_s^m(\varepsilon)\Big) m^i = \sum_{m\in M} \lambda_1^m(\varepsilon) m^i = \sum_{m\in M} c_m m^i = c(m^i). \ \square$$

Zauważmy, że przyjmując w twierdzeniu 4.2 $M = \{1\} \subseteq R = \mathbf{Q}$, $A = \{a\}$ i $G = E$ otrzymamy, jako wniosek, lemat Burnside'a. Z kolei twierdzenia 4.2 dowodzi się używając wielokrotnie lematu Burnside'a w dość specyficznej sytuacji. Zatem udowodnione twierdzenie jest w istocie równoważną formą lematu. Można też sformułować i udowodnić — bezpośrednio, albo jako wniosek z twierdzenia 4.2 — „wagową" formę lematu Burnside'a, co pozostawiamy Czytelnikowi.

Policzmy dla przykładu szereg Ω dla naszyjników o pięciu paciorkach białych lub czarnych (nie białych), to znaczy dla orbit w zbiorze funkcji $\{1, 2\}^{\{1,2,3,4,5\}}$, na którym działa z prawej strony grupa D_5. Obierając $R = \mathbf{Q}[b, n]$ i $M =$

$= \{b, n, b^2, n^2, b^3, n^3, \ldots\}$ oraz $w(1) = b$, $w(2) = n$ otrzymujemy $c(b, n) = b+n$. Podstawiając do indeksu cyklowego grupy D_5, który jest wielomianem

$$\tfrac{1}{10}(x_1^5 + 5x_1x_2^2 + 4x_5),$$

mamy

$$\Omega = \tfrac{1}{10}\big((b+n)^5 + 5(b+n)(b^2+n^2) + 4(b^5+n^5)\big) =$$
$$= b^5 + b^4n + 2b^3n^2 + 2b^2n^3 + bn^4 + n^5,$$

w pełnej zgodności z rys. 25.

Rozważmy teraz funkcje ze zbioru $\mathscr{P}_2(A)$, gdzie A jest zbiorem n-elementowym, w zbiór $N_0 = \{0, 1, 2, \ldots\}$. Wagą niech będzie funkcja $w\colon N_0 \to M = \{1, t, t^2, \ldots\} \subseteq Q[t]$, gdzie $w(k) = t^k$ dla $k \in N_0$. Ograniczając się do funkcji o wartościach 0 i 1 otrzymamy jako funkcję wagi t^k graf o n wierzchołkach i k krawędziach. Jeżeli zaś będziemy rozważali dowolne funkcje, to odpowiadają im tak zwane *multigrafy* ($f(a, b) = f(b, a) = l$, jeżeli pomiędzy wierzchołkami a i b jest l krawędzi). Wobec powyższego szereg g_n przeliczający grafy o n wierzchołkach zgodnie z liczbą ich krawędzi wygląda następująco:

$$g_n(t) = Z(S_n^{(2)};\ 1+t).$$

Podobny szereg dla multigrafów jest zadany wzorem

$$m_n(t) = Z(S_n^{(2)};\ 1+t+t^2+\ \ldots) = Z\big(S_n^{(2)};\ (1-t)^{-1}\big).$$

W szczególności otrzymujemy dla $n = 4$

$$g_4(t) = 1 + t + 2t^2 + 3t^3 + 2t^4 + t^5 + t^6$$

i

$$m_4(t) = 1 + t + 3t^2 + 6t^3 + 11t^4 + 18t^5 + 32t^6 + 48t^7 + \ \ldots$$

Wartości współczynników ostatniego szeregu zostały zaczerpnięte z książki Harary'ego i Palmera [1]. Tamże można znaleźć przykłady zastosowania twierdzenia 4.2 do wyznaczania liczby grafów o krawędziach pomalowanych na wzajemnie zamienialne kolory i do obliczania liczby automatów skończonych. W istocie rzeczy znaczna część książki Harary'ego i Palmera [1] jest poświęcona zastosowaniom różnych wersji przedstawianych tu metod.

Następujący przykład pochodzi w zasadzie of Pólyi. Dane są dwie kule białe, jedna czarna i trzy zielone. Znaleźć liczbę sposobów rozmieszczenia tych kul w wierzchołkach ośmiościanu foremnego, jeżeli ośmiościan można obracać. Jak stwierdziliśmy w paragrafie 3 odpowiedni indeks cyklowy ma postać

$$\tfrac{1}{24}(x_1^6 + 6x_1^2x_4 + 3x_1^2x_2^2 + 6x_2^3 + 8x_3^2).$$

Niech R będzie pierścieniem wielomianów trzech zmiennych b, n i z takich, że $b^3 = n^2 = z^4 = 0$. (Ściślej, R jest izomorficzny z $Q[b, n, z]/(b^3, n^2, z^4)$). Niech waga $w\colon \{0, 1, 2\} \to R$ będzie określona przez równości $w(0) = b$, $w(1) = n$, $w(2) =$

$= z$. Wówczas żądane rozkłady są orbitami funkcji ze zbioru wierzchołków A ośmiościanu w zbiór $\{0, 1, 2\}$ mającymi wagę b^2nz^3. Wagą wszelkich pozostałych funkcji jest zero. Wobec tego szukana liczba jest jedynym niezerowym współczynnikiem w wyrażeniu

$$\tfrac{1}{24}\left((b+n+z)^6+6(b+n+z)^2\cdot 0+3(b+n+z)^2(b^2+z^2)^2+6(b^2+z^2)^3+8(z^3)^2\right) =$$

$$= \tfrac{1}{24}\left(\frac{6!}{2!\,1!\,3!}b^2nz^3+6nz\cdot 2b^2z^2\right) = \left(\frac{5\cdot 6}{2\cdot 2\cdot 3}+\frac{12}{24}\right)b^2nz^3 = 3b^2nz^3.$$

Jeżeli kulki różnych kolorów będą reprezentowały różne atomy, a ośmiościan strukturę molekuły związku chemicznego, to opisana technika pozwala na odnalezienie liczby związków chemicznych o tym samym wzorze liniowym, lecz o innej budowie cząsteczki, a więc tak zwanych izomerów. Właśnie temu problemowi była poświęcona oryginalna praca Pólya [1].

Zwróćmy uwagę, że jeżeli A jest G-zbiorem, to wybierając dla różnych elementów zbioru B różne wagi ze zbioru $M = \{t_1, t_2, \ldots\}$, gdzie t_i są „zmiennymi" w pierścieniu „wielomianów" $Q[t_1, t_2, \ldots]$, w którym $t_i^2 = 0$ dla każdego i, a następnie podstawiając $t_1+t_2+\ldots$ do $Z(G, A)$, otrzymamy liczbę orbit różnowartościowych funkcji z A do B.

Przyjmując w szczególności za A zbiór ścian sześcianu, za B zbiór $\{1, 2, 3, 4, 5, 6\}$ i za G grupę obrotów sześcianu, znajdziemy, ile jest różnych kostek do gry. Wobec tego mamy tych kostek k, gdzie

$$kt_1t_2t_3t_4t_5t_6 = Z(G, A; t_1+t_2+t_3+t_4+t_5+t_6).$$

Podstawiając mamy $k = 6!/4! = 30$.

Jednakże przepisowa kostka do gry powinna mieć sumę oczek na przeciwległych ściankach równą siedem. Wobec tego odpowiada ona funkcji różnowartościowej ze zbioru $\{1, 2, 3\}$ w zbiór ścian sześcianu, przy czym obrazy różnych elementów nie mogą tworzyć pary ścian przeciwległych. Ponadto dwie kostki są takie same, jeżeli jedną funkcję można otrzymać z drugiej przez złożenie z obrotem.

Naturalna metoda rozwiązania tego zadania polega na przypisaniu parom ścian przeciwległych różnych wag. Jednakże nie można tego uczynić, gdyż twierdzenie 4.2 wymaga, ażeby waga była funkcją stałą na orbitach. Jest to kłopot często spotykany w zastosowaniach.

Zwróćmy jednakże uwagę na to, że w dowodzie twierdzenia 4.2 naprawdę istotne było jedynie to, że funkcja w^* jest stała na $G\times H$-orbitach w zbiorze funkcji. Jedyna różnica będzie teraz polegała na tym, że czynnik wyrażenia $\lambda(\alpha, \beta)$ odpowiadający elementowi a z α-cyklu długości k zostanie zastąpiony wyrażeniem

$$w(b)w(\beta b)\ldots w(\beta^{k-1}b),$$

gdzie b jest punktem stałym operatora β^k. Modyfikacja ta prowadzi do następującego twierdzenia.

TWIERDZENIE 4.4. *Niech A, B, G, H i M będą jak w twierdzeniu 4.2 i niech $w\colon B \to M$ będzie funkcją taką, iż funkcja $w^*\colon B^A \to M$ określona wzorem*

$$w^*(f) = \prod_{a \in A} w(f(a))$$

jest funkcją stałą na $G \times H$-orbitach zbioru B^A. Wówczas szereg Ω przeliczający orbity funkcji zgodnie z ich w^*-wagami jest równy

$$|H|^{-1} \sum_{\beta \in H} Z(G, A; p_1(\beta), p_2(\beta), \ldots, p_{|A|}(\beta)),$$

gdzie

$$p_i(\beta) = \sum_{b:b=\beta^i b} w(b) w(\beta b) \ldots w(\beta^{k-1} b),$$

$i = 1, \ldots, |A|$, ($p_i(\beta) = 0$, *jeżeli operator* β^i *nie ma punktów stałych*). □

Zastosujmy to twierdzenie do problemu przepisowych kostek do gry. Niech $A = \{1, 2, 3\}$, niech B będzie zbiorem ścian sześcianu, niech $G = E$, niech H będzie grupą obrotów sześcianu i niech $M = \{t_1, t_2, t_3\} \subseteq \mathbf{Q}[t_1, t_2, t_3]$, gdzie $t_1^2 = t_2^2 = t_3^2 = 0$. Funkcję w zdefiniujemy przypisując różnym parom przeciwległych ścian sześcianu różne elementy z M. Funkcja w^* na funkcji f przyjmuje wartość $t_1 t_2 t_3$, gdy f odpowiada przepisowej kostce i ma wartość zero w pozostałych przypadkach. Zatem w^* jest wagą. $Z(G, A) = x_1^3$, czyli musimy odnaleźć tylko szeregi $p_1(\beta)$ dla tych β, które mają punkty stałe. Kolejno znajdujemy $2(t_1+t_2+t_3)$, $2t_1$, $2t_2$, $2t_3$. Wobec tego szukanym szeregiem jest

$$\tfrac{8}{24}\left((t_1+t_2+t_3)^3 + t_1^3 + t_2^3 + t_3^3\right) = \frac{8 \cdot 3!}{24} t_1 t_2 t_3 = 2 t_1 t_2 t_3.$$

Zatem są tylko dwie przepisowe kostki.

Odnotujmy jeszcze jeden użyteczny fakt.

TWIERDZENIE 4.5 (de Bruijn). *Niech wszystkie oznaczenia będą jak w twierdzeniu 4.4, niech $w\colon B \to M$ będzie dowolną funkcją i niech β będzie ustalonym operatorem z grupy H. Wówczas suma wag Ω wszystkich funkcji $f \in B^A$ takich, że $\beta f = f$ jest równa* $Z(G, A; p_1(\beta), p_2(\beta), \ldots, p_{|A|}(\beta))$.

Dowód. Rozważmy zbiór $F = \{f \in B^A\colon \beta f = f\}$. Funkcja m jest wagą na zbiorze F, na którym działa z lewej strony grupa G poprzez $\alpha f = f\alpha^{-1}$. Jeżeli o_m oznacza liczbę orbit wagi m w G-zbiorze F, to z lematu Burnside'a otrzymujemy

$$\Omega = \sum_{m \in M} o_m m = \frac{1}{|G|} \sum_{\alpha \in G} \lambda(\alpha, \beta),$$

gdzie $\lambda(\alpha, \beta)$ jest szeregiem przeliczającym zgodnie z wagami funkcje z F takie, że $f\alpha^{-1} = f$, a więc takie, że $\beta f \alpha^{-1} = f$. Dalsza część dowodu jest powtórzeniem dowodu poprzedniego twierdzenia. □

Stosując powyższe twierdzenie w sytuacji, gdy zbiór B^A jest zbiorem funkcji ze zbioru $\mathscr{P}_2(A)$ w zbiór $\{0, 1\}$, grupa G jest grupą permutacji na A, β zaś cyklicznym przestawieniem 0 i 1, otrzymamy szereg przeliczający zgodnie z wagami grafy o wierzchołkach ze zbioru A, które są izomorficzne ze swoim uzupełnieniem. Przyjmując $w\colon \{0, 1\} \to \mathbf{Q}[t]$, $w(0) = 1$, $w(1) = t$, otrzymujemy t^k jako wagę grafu o k krawędziach. Łatwo sprawdzić, że $p_1(\beta) = p_3(\beta) = \ldots = 0$, $p_2(\beta) = 2t$, $p_4(\beta) = 2t^2, \ldots$ Wobec tego poszukiwanym szeregiem jest

$$Z(S_n^{(2)};\ 0, 2t, 0, 2t^2, 0, 2t^3, \ldots).$$

Graf o n wierzchołkach, który jest izomorficzny ze swym uzupełnieniem, musi mieć $n(n-1)/4$ krawędzi. Zatem poszukiwana liczba jest jedynym niezerowym współczynnikiem w powyższym szeregu, o ile $n(n-1)/4$ jest liczbą całkowitą, i zerem w przeciwnym przypadku. Wobec tego mamy

$$Z(S_n^{(2)};\ 0, 2, 0, 2, \ldots)$$

samouzupełnialnych grafów o n wierzchołkach.

Zadania

1. Uzasadnić, iż relacja „być takim samym" w G-zbiorze A jest relacją równoważności wyznaczoną przez podział zbioru A na orbity.

2. Udowodnić, że liczba istotnie różnych sposobów przypisania n etykiet n wierzchołkom grafu Γ jest równa $n!|G|^{-1}$, gdzie G jest grupą automorfizmów grafu Γ.

3. Znaleźć liczbę pokolorowań na co najwyżej k kolorów n-miejscowej ruletki, tzn. tarczy koła obracającego się na osi przechodzącej przez środek i podzielonej na n jednakowych sektorów. Znaleźć liczbę pokolorowań na dokładnie k kolorów.

Wskazówka: Wykorzystać indeks cykliczny grupy cyklicznej $Z(C_n)$.

4. Udowodnić, że samouzupełnialnych grafów o n wierzchołkach jest

$$Z(S_n^{(2)};\ 0, 2, 0, 2, \ldots)$$

wykorzystując metodę naszkicowaną w paragrafie 3.

5. Korzystając z metod tego rozdziału udowodnić, że jest dokładnie c_{nk} permutacji o k cyklach w grupie S_n, gdzie $\sum_{k=0}^{n} c_{nk}x^k = [x]^n = x(x+1)(x+n-1)$, to znaczy, że $c_{nk} = |s(n, k)|$ (bezwzględna wartość liczby Stirlinga pierwszego rodzaju — por. rozdział 1, § 4).

Wskazówka: Wobec lematu Burnside'a lub wniosku 2.2 n nierozróżnialnych przedmiotów można umieścić w m ponumerowanych pudełkach na $\frac{1}{n!}\sum_{k=0}^{n} c_{nk}m^k$ sposobów, a z drugiej strony liczba ta jest równa $\binom{m+n-1}{n}$.

6. Dane są trzy kulki białe, jedna czarna i dwie zielone. Na ile sposobów można je umieścić w trzech ponumerowanych pudełkach tak, aby każde z pudełek zawierało (a) po dwie kulki, (b) co najwyżej trzy kulki. Znaleźć odpowiedź w sytuacji, gdy pierwsze dwa pudełka są nierozróżnialne i gdy wszystkie trzy są nierozróżnialne.

7. Ile jest czworościennych kostek do gry? Ile jest ośmiościennych? Ile jest prawidłowych ośmiościennych kostek, to znaczy takich, że suma oczek na przeciwległych ścianach wynosi 9?

8. (Tomescu). Oznaczmy przez C_2 multyplikatywną grupę liczb całkowitych złożoną z 1 i -1. Grupa C_2^n działa na zbiorze B_n funkcji boolowskich n zmiennych w następujący sposób: jeżeli $\langle \alpha_1, \alpha_2, \dots, \alpha_n \rangle \in C_2^n$ i $f \in B_n$, to

$$\alpha f = f(y_2^{\alpha_1}, y_2^{\alpha_2}, \dots, y_n^{\alpha_n}),$$

gdzie $y_i^1 = y_i$, $y_i^{-1} = \neg y_i$, $i = 1, 2, \dots, n$.

Wykazać, że w zbiorze $\{f \in B_n \colon |f^{-1}(1)| = k\}$ liczba C_2^n-orbit jest równa

$$\frac{1}{2^n}\binom{2^n}{k}, \qquad \text{jeżeli } k \equiv 1 \pmod 2,$$

i

$$\frac{1}{2^n}\left[\binom{2^n}{k} + (2^n - 1)\binom{2^{n-1}}{k/2}\right], \qquad \text{jeżeli } k \equiv 0 \pmod 2,$$

oraz że liczba C_2^n-orbit w zbiorze B_n jest równa

$$\frac{1}{2^n}\left(2^{2^n} + (2^n - 1)2^{2^{n-1}}\right).$$

Wskazówka: Znaleźć $Z(C_2^n, B_n)$ i znaleźć współczynnik przy t^k w szeregu $Z(C_2^n, B_n; 1+t, 1+t^2)$ oraz $Z(C_2^n, B_n; 2, 2)$.

9 (Lehmann). Niech grupa G działa na zbiorze A, a grupa H na zbiorze B. Zdefiniujmy działanie grupy $G \times H^A$ na zbiorze B^A przyjmując

$$[\langle \alpha, \varphi \rangle f](a) = \varphi(a) f(\alpha^{-1} a),$$

gdzie $\langle \alpha, \varphi \rangle \in G \times H^A$, $f \in B^A$ i $a \in A$. Oznaczmy przez $c(\alpha)$ liczbę α-cykli na A i niech a_i będzie reprezentantem α-cyklu długości k_i, $i = 1, 2, \dots, c(\alpha)$. Definiujemy

$$\beta_i(\alpha, \varphi) = \varphi(a_i)\varphi(\alpha^{-1} a_i) \dots \varphi(\alpha^{-k_i+1} a_i) \in H.$$

Udowodnić, że jeżeli funkcja $w \colon B \to M$ jest wagą na H-zbiorze B, to funkcja $w^* \colon B^A \to M$, gdzie $w^*(f) = \prod_{a \in A} w(f(a))$, jest wagą na $G \times H^A$-zbiorze B^A, i jeżeli o_m oznacza liczbę orbit funkcji wagi m, $m \in M$, to

$$\Omega = \sum_m o_m \cdot m = \frac{1}{|G| \cdot |H|^{|A|}} \sum_{\langle \alpha, \varphi \rangle \in G \times H^A} \prod_{i=1}^{c(\alpha)} \sum_b w(b)^{k_i},$$

gdzie suma w każdym czynniku przebiega po wszystkich należących do B punktach stałych operatora $\beta_i(\alpha, \varphi)$.

(Obraz grupy $G \times H^A$ w grupie permutacji zbioru B^A, przy opisanym powyżej działaniu, nazywa się *iloczynem wieńcowym* grup G i H.)

KONFIGURACJE KOMBINATORYCZNE

Wyobraźmy sobie, że w zawodach żużlowych startuje 16 zawodników. Zawody składają się z pewnej liczby biegów, w każdym z których występuje czterech zawodników. Aby szanse wszystkich zawodników były równe, chcemy tak zaplanować biegi, aby każda para (nieuporządkowana) zawodników spotykała się w dokładnie jednym biegu. Wszystkich takich par jest $\binom{16}{2} = 120$, w każdym zaś biegu spotyka się $\binom{4}{2} = 6$ par. Jeśli więc rozstawienie o tej własności istnieje, to liczba biegów musi być równa $b = 120/6 = 20$. Jednakże istnienie takiego rozstawienia zawodników nie jest bynajmniej oczywiste. Formułując nasz problem bardziej abstrakcyjnie możemy powiedzieć, że szukamy rodziny $(B_1, \ldots, B_{20})$ podzbiorów 4-elementowych zbioru 16-elementowego X, o tej własności, iż każda para nieuporządkowana $\{x, y\} \subseteq X$ jest zawarta w dokładnie jednym spośród zbiorów B_i, $1 \leqslant i \leqslant 20$. Rodzina taka nazywa się konfiguracją o parametrach $v = 16$, $k = 4$, $\lambda = 1$.

Głównym zagadnieniem rozważanym w tym rozdziale będzie problem istnienia i konstrukcji konfiguracji dla danych wartości parametrów. Okaże się, na przykład, że konfiguracja o parametrach $v = 16$, $k = 4$, $\lambda = 1$ istnieje (p. § 6). Omawiane będą też pewne zagadnienia pokrewne, związane ze skończonymi płaszczyznami rzutowymi, zbiorami różnicowymi, ortogonalnymi kwadratami łacińskimi oraz macierzami Hadamarda. Będziemy zajmowali się również kwadratami Rooma — obiektami kombinatorycznymi związanymi z planowaniem rozgrywek brydżowych.

§ 1. Konfiguracje: podstawowe własności

Niech X będzie zbiorem skończonym, $\mathscr{B} = (B_1, \ldots, B_b)$ zaś pewną rodziną jego podzbiorów. Elementy $x \in X$ będziemy nazywali *punktami*, a zbiory B_i *blokami*.

Parę $\langle X, \mathscr{B}\rangle$ nazwiemy *konfiguracją* o parametrach v, k, λ, jeśli spełnione są następujące warunki:

K1. $|X| = v$.

K2. $|B_i| = k$ dla $1 \leqslant i \leqslant b$.

K3. Każdy 2-elementowy zbiór $\{x, y\} \subseteq X$ jest podzbiorem dokładnie λ bloków spośród $B_1, \ldots, B_b$.

K4. $\lambda > 0$ oraz $k < v-1$.

Ostatni warunek wyklucza pewne zdegenerowane przypadki. Zauważmy, że nie żądamy, by wszystkie bloki były różne. Warunki K2, K3 wyrażają fakt, iż w pewnym sensie punkty są „rozmieszczone regularnie" w blokach. Okazuje się, że pociągają one za sobą jeszcze jeden warunek tego typu. Istotnie, ustalmy pewien punkt x i rozważmy $v-1$ zbiorów $\{x, y\}$, $y \in X \setminus \{x\}$. Policzmy liczbę wystąpień tych zbiorów w blokach, tzn. liczbę par $\langle \{x, y\}, B_i\rangle$ takich, że $\{x, y\} \subseteq B_i$. Z jednej strony, na mocy K3, każdy zbiór $\{x, y\}$ jest zawarty w λ blokach, naszych par jest więc $(v-1)\lambda$. Z drugiej strony, jeśli x występuje w r blokach, to w każdym z nich tworzy $k-1$ zbiorów $\{x, y\}$. Zatem licząc „blokami" otrzymujemy wynik $r(k-1)$. Z równości

(1.1) $$\lambda(v-1) = r(k-1)$$

wynika, że r jest wyznaczone przez parametry v, k, λ, a więc nie zależy od wyboru punktu x.

WNIOSEK 1.1. *Każdy punkt konfiguracji występuje w dokładnie r blokach, gdzie*

(1.2) $$r = \frac{\lambda(v-1)}{k-1}. \qquad \square$$

Jeśli policzymy na dwa sposoby liczbę wystąpień punktów w blokach, tzn. liczbę par postaci $\langle x, B_i\rangle$, gdzie $x \in B_i$, to otrzymamy

(1.3) $$vr = bk,$$

czyli

(1.4) $$b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)}.$$

Liczba bloków konfiguracji jest więc jednoznacznie wyznaczone przez parametry v, k, λ.

Podstawowym problemem teorii konfiguracji jest zbadanie, dla jakich parametrów konfiguracje istnieją. Problem ten jest bardzo złożony i — jak na razie — daleki od całkowitego rozwiązania. Będziemy mówili, że konfiguracje $\langle X, \mathscr{B}\rangle$ i $\langle Y, \mathscr{C}\rangle$ są *izomorficzne*, jeśli istnieją wzajemnie jednoznaczne odwzorowania

$\varphi: X \to Y$ oraz $\psi: \mathscr{B} \to \mathscr{C}$ takie, że

(1.5) $$x \in B \Leftrightarrow \varphi(x) \in \psi(B)$$

dla każdego punktu $x \in X$ i bloku $B \in \mathscr{B}$. Definicja ta ma sens jedynie w przypadku, gdy żadna z konfiguracji $\langle X, \mathscr{B} \rangle$, $\langle Y, \mathscr{C} \rangle$ nie zawiera powtarzających się bloków, nie bardzo bowiem wiadomo, co to jest „odwzorowanie pomiędzy zbiorami z powtórzeniami". Gdy mówimy o izomorfiźmie konfiguracji o powtarzających się blokach, należy w obu konfiguracjach wszystkie bloki traktować jako obiekty różne, relację $\in$ zaś jako abstrakcyjną *relację incydencji* pomiędzy punktami a blokami – wtedy dwa różne bloki mogą być incydentne z tymi samymi punktami.

W szczególnym przypadku, gdy $X = Y$, $\mathscr{B} = \mathscr{C}$, o parze $\alpha = \langle \varphi, \psi \rangle$ spełniającej warunek (1.5) będziemy mówili, że wyznacza *automorfizm* konfiguracji $\langle X, \mathscr{B} \rangle$. Funkcje φ, ψ są wtedy permutacjami odpowiednio zbioru punktów i zbioru bloków – będziemy je nazywali *działaniem automorfizmu α na punktach* oraz *działaniem automorfizmu α na blokach*. Zamiast $\varphi(x)$, $\psi(B)$ będziemy też pisali $(x)\alpha$, $(B)\alpha$. Jest oczywiste, że zbiór wszystkich automorfizmów ustalonej konfiguracji tworzy grupę, jeśli złożenie $\alpha\beta$ automorfizmów α i β zdefiniujemy następująco: $(x)\alpha\beta = ((x)\alpha)\beta$, $(B)\alpha\beta = ((B)\alpha)\beta$. Zaleta pisania $(x)\alpha$, $(B)\alpha$ zamiast $\alpha(x)$, $\alpha(B)$ jest tu widoczna.

Zauważmy jeszcze, że jeśli wszystkie bloki konfiguracji są różne, to dowolny automorfizm jest jednoznacznie wyznaczony przez jego działanie na punktach konfiguracji.

Wygodnym sposobem reprezentowania rodziny podzbiorów ustalonego zbioru, w szczególności konfiguracji $\langle X, \mathscr{B} \rangle$, gdzie $X = \{x_1, \ldots, x_v\}$, $\mathscr{B} = (B_1, \ldots, B_b)$, jest jej *macierz incydencji*. Definiujemy ją jako macierz $A = [a_{ij}]$ o v wierszach odpowiadających punktom i b kolumnach odpowiadających blokom, gdzie

$$a_{ij} = \begin{cases} 1, & \text{jeśli } x_i \in B_j, \\ 0, & \text{jeśli } x_i \notin B_j. \end{cases}$$

Na mocy K2 i wniosku 1.1 każda kolumna macierzy A zawiera k jedynek, a każdy wiersz r jedynek.

Oczywiście macierz incydencji wyznacza konfigurację z dokładnością do izomorfizmu. Co więcej, dwie konfiguracje o macierzach incydencji A i B są izomorficzne wtedy i tylko wtedy, gdy B można otrzymać z A przez permutację kolumn i wierszy.

PRZYKŁAD. (a) Niech

$$X = \{1, 2, \ldots, 7\},$$
$$\mathscr{B} = (\{1, 2, 4\}, \{2, 3, 5\}, \{3, 4, 6\}, \{4, 5, 7\}, \{1, 5, 6\}, \{2, 6, 7\}, \{1, 3, 7\}).$$

Wówczas $\langle X, \mathscr{B} \rangle$ jest konfiguracją o parametrach $v = 7$, $k = 3$, $\lambda = 1$, $r = 3$,

$b = 7$ i o macierzy incydencji

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

(b) Niech $2 < k+1 < v = |X|$ i niech $\mathscr{B} = \mathscr{P}_k(X)$. Wówczas $\langle X, \mathscr{B} \rangle$ jest konfiguracją o parametrach

$$b = \binom{v}{k}, \quad r = \binom{v-1}{k-1}, \quad \lambda = \binom{v-2}{k-2}.$$

Warunek K3 wraz z wnioskiem 1.1 można wyrazić w postaci macierzowej następująco:

(1.6) $$AA^T = (r-\lambda)I_v + \lambda J_v,$$

gdzie I_v jest macierzą jednostkową, J_v zaś macierzą złożoną z samych jedynek, obie wymiaru $v \times v$. Zwykle zamiast I_v, J_v będziemy pisali I, J.

LEMAT 1.2. *Niech* $B = (r-\lambda)I + \lambda J$. *Wówczas*

$$\det B = (r-\lambda)^{v-1}(v\lambda - \lambda + r).$$

Dowód. Mamy

$$B = \begin{bmatrix} r & \lambda & \dots & \lambda \\ \lambda & r & \dots & \lambda \\ \dots & \dots & \dots & \dots \\ \lambda & \lambda & \dots & r \end{bmatrix}.$$

Aby obliczyć wyznacznik, odejmujemy pierwszą kolumnę od pozostałych, a następnie dodajemy do pierwszego wiersza powstałej macierzy wszystkie pozostałe wiersze. Operacje te nie zmieniają wartości wyznacznika. Otrzymana macierz ma same zera ponad główną przekątną oraz wartości $r+(v-1)\lambda$, $r-\lambda$, ..., $r-\lambda$ na przekątnej. Stąd $\det B = \big(r+(v-1)\lambda\big)(r-\lambda)^{v-1}$. □

TWIERDZENIE 1.3 (nierówność Fishera). *W dowolnej konfiguracji o parametrach* v, k, λ, r, b

(1.7) $$b \geqslant v,$$

i w konsekwencji

(1.8) $$r \geqslant k.$$

Dowód. Załóżmy, że A jest macierzą incydencji pewnej konfiguracji, w której $b < v$. Dodając do A $v-b$ kolumn zerowych otrzymujemy wtedy macierz kwadratową $\bar{A}$ wymiaru $v \times v$ taką, że

$$\bar{A}\bar{A}^T = AA^T = (r-\lambda)I + \lambda J.$$

Z jednej strony $\det \bar{A} = 0$, gdyż $\bar{A}$ zawiera kolumnę złożoną z samych zer, z drugiej zaś strony, na mocy lematu 1.2 oraz równości $\det(\bar{A}\bar{A}^T) = (\det \bar{A})^2$, mamy

$$(\det \bar{A})^2 = (r-\lambda)^{v-1}(v\lambda - \lambda + r) \neq 0,$$

gdyż wobec wzoru (1.1) równość $r = \lambda$ pociągałaby za sobą $v = k$, wbrew K4. Tak więc nie może być $b < v$. Nierówność (1.8) otrzymujemy z (1.7) i (1.3). □

Zreasumujmy poznane dotychczas konieczne warunki istnienia konfiguracji:

Twierdzenie 1.4. *Jeśli konfiguracja o parametrach v, k, λ istnieje, to*

$$\lambda(v-1) \equiv 0 \,(\mathrm{mod}\, k-1), \tag{1.9}$$

$$\lambda v(v-1) \equiv 0 \,(\mathrm{mod}\, k(k-1)), \tag{1.10}$$

$$\lambda(v-1) \geqslant k(k-1). \tag{1.11}$$

Dowód. Kongruencje (1.9) i (1.10) wynikają z (1.2) i (1.4), jako że liczby $r = \lambda(v-1)/(k-1)$ i $b = \lambda v(v-1)/(k(k-1))$ muszą być całkowite. Nierówność (1.11) jest równoważna nierówności Fishera. □

Niestety, powyższe warunki nie są wystarczające dla istnienia konfiguracji o danych parametrach. Co więcej, nie jest znana żadna pełna charakteryzacja „realizowanych" parametrów.

Wiadomo jednak, że jeśli $k \leqslant 5$, to zależności (1.9), (1.10) (wraz z warunkiem K4) są wystarczające dla istnienia konfiguracji, z wyjątkiem przypadku parametrów $v = 15$, $k = 5$, $\lambda = 2$, dla których konfiguracja nie istnieje. Fakt ten udowodniony został przez H. Hananiego, przy czym pewne szczególne przypadki znane już były znacznie wcześniej. Dowód jest zbyt skomplikowany, by go tu przytoczyć (p. Hanani [4]), ograniczymy się więc jedynie do rozważenia w § 11 przypadku $k = 3$, $\lambda = 1$. Warto jeszcze dodać, że R. M. Wilson [1,2,3] udowodnił, iż dla dowolnych ustalonych k, λ warunki (1.9), (1.10) są wystarczające dla istnienia konfiguracji, jeśli v jest dostatecznie duże.

Teoria konfiguracji była rozwijana początkowo w związku ze statystyczną teorią planowania eksperymentów. Stąd też większość prac na ich temat, szczególnie tych wcześniejszych, była publikowana w czasopismach statystycznych, a jeden z pierwszych rezultatów teorii konfiguracji (twierdzenie 1.3) związany jest z nazwiskiem wybitnego statystyka R. A. Fishera. Warto pokrótce wspomnieć, na czym polega związek pomiędzy teorią konfiguracji i planowaniem eksperymentów.

W tym celu wyobraźmy sobie, że grupa 7 degustatorów ma za zadanie porównać 7 gatunków koniaków. Najprostszym rozwiązaniem byłaby degustacja wszystkich gatunków przez każdego degustatora, jednakże wtedy możliwość

uzyskania odpowiedniego stopnia koncentracji stałaby pod znakiem zapytania. Załóżmy więc, że każdy z degustatorów próbuje co najwyżej 3 gatunki. Aby porównanie było jak najrzetelniejsze, żądamy, by

(1) Każdy degustator próbował tę samą liczbę gatunków,

(2) Każda para gatunków porównywana była przez tę samą liczbę degustatorów.

Aby to osiągnąć, wystarczy rozważyć konfigurację z przykładu (a), w której punkty odpowiadają gatunkom (ang. *varieties*, stąd pozostał zwyczaj oznaczania liczby punktów przez v), bloki zaś odpowiadają degustatorom. Więcej szczegółów na temat tego typu zagadnień można znaleźć w klasycznej monografii Fishera [2].

Innym ważnym zastosowaniem konfiguracji, o którym będziemy mówić w rozdziale 8, jest teoria kodów.

§ 2. Konfiguracje kwadratowe, skończone płaszczyzny rzutowe

Ważną klasę stanowią konfiguracje o liczbie punktów równej liczbie bloków. Będziemy je nazywali *konfiguracjami kwadratowymi*. Z równości $vr = bk$ wynika, iż dla dowolnej konfiguracji kwadratowej mamy oprócz $v = b$ również $r = k$.

Równanie (1.1) przyjmuje więc postać

(2.1) $$\lambda(v-1) = k(k-1).$$

Okazuje się, że w konfiguracji kwadratowej rola punktów i bloków jest symetryczna*: nie tylko każde dwa punkty są zawarte w dokładnie λ blokach, lecz również każde dwa bloki zawierają dokładnie λ wspólnych punktów:

TWIERDZENIE 2.1. *Jeśli $\langle X, \mathscr{B}\rangle$, gdzie $\mathscr{B} = (B_1, \ldots, B_v)$, jest konfiguracją kwadratową o parametrach v, k, λ, to*

(2.2) $$|B_i \cap B_j| = \lambda$$

dla dowolnych $i \neq j$, $1 \leqslant i, j \leqslant v$.

Dowód. Macierz incydencji A konfiguracji kwadratowej $\langle X, \mathscr{B}\rangle$ spełnia równanie

(2.3) $$AA^T = (k-\lambda)I + \lambda J$$

(gdyż $r = k$). Mamy poza tym

$$AJ = kJ,$$

gdyż każdy wiersz macierzy A zawiera k jedynek, oraz

$$JA = kJ,$$

* Dlatego też konfiguracje kwadratowe nazywane są również *konfiguracjami symetrycznymi*.

gdyż każda kolumna macierzy A zawiera k jedynek. Tak więc $AJ = JA$. Z lematu 1.2 wynika, że $\det A \neq 0$, a więc

(2.4) $$A^T A = A^{-1} A A^T A = A^{-1}[(k-\lambda)I + \lambda J]A = (k-\lambda)I + \lambda A^{-1} J A = \\ = (k-\lambda)I + \lambda A^{-1} A J = (k-\lambda)I + \lambda J.$$

Lecz ta ostatnia równość to nic innego jak macierzowa postać równości (2.2). □

Porównując (2.3) z (2.4) widzimy, że dla macierzy incydencji konfiguracji kwadratowej spełniona jest równość $AA^T = A^T A$. Macierz kwadratową o tej własności nazywamy *normalną*.

Twierdzenie 2.1 można również wyrazić w następujący sposób: jeśli A jest macierzą incydencji konfiguracji kwadratowej, to A^T jest macierzą incydencji pewnej konfiguracji o tych samych parametrach, tzw. *konfiguracji dualnej*. Z naszych rozważań wynika, że każda konfiguracja kwadratowa $\langle X, \mathscr{B}\rangle$, gdzie $\mathscr{B} = (B_1, \ldots, B_v)$, spełnia następujące warunki:

KK1. $|B_i| = k$ dla $1 \leqslant i \leqslant v$.

KK2. $|B_i \cap B_j| = \lambda$ dla $1 \leqslant i < j \leqslant v$.

KK3. $\lambda > 0$ oraz $k < v-1$.

Okazuje się, że warunki te w pełni charakteryzują konfiguracje kwadratowe:

TWIERDZENIE 2.2. *Niech $\mathscr{B} = (B_1, \ldots, B_v)$ będzie rodziną podzbiorów zbioru v-elementowego X spełniającą warunki* KK1, KK2, KK3. *Wówczas $\langle X, \mathscr{B}\rangle$ jest konfiguracją kwadratową o parametrach v, k, λ.*

Dowód. Wykażemy najpierw, że każdy punkt występuje w dokładnie k blokach. Niech $A = [a_{ij}]$ będzie macierzą incydencji dla $\langle X, \mathscr{B}\rangle$. Mamy wykazać, że $AJ = kJ$. Warunki KK1 i KK2 możemy zapisać w postaci macierzowej jako

(2.5) $$JA = kJ,$$

(2.6) $$A^T A = (k-\lambda)I + \lambda J.$$

Na mocy lematu 1.2 A jest macierzą nieosobliwą, możemy więc obie strony równości (2.5) pomnożyć prawostronnie przez A^{-1}. Otrzymujemy wtedy

(2.7) $$JA^{-1} = k^{-1} J.$$

Mamy poza tym

$$JA^T A = J[(k-\lambda)I + \lambda J] = (k-\lambda+\lambda v)J.$$

Mnożąc prawostronnie przez A^{-1} i korzystając z (2.7) otrzymujemy

$$JA^T = (k-\lambda+\lambda v)k^{-1} J,$$

co oznacza, że suma elementów każdego wiersza macierzy A jest taka sama (i wynosi $(k-\lambda+\lambda v)k^{-1}$). Lecz skoro wszystkich jedynek macierzy A jest kv, to suma ta jest równa $kv/v = k$. Tak więc A^T jest macierzą incydencji pewnej

konfiguracji kwadratowej o parametrach v, k, λ. W myśl twierdzenia 2.1 A odpowiada konfiguracji o tych samych parametrach. □

Warto zauważyć, że w przypadku macierzy zero-jedynkowych równość (2.5) wynika z (2.6). Macierz zero-jedynkowa A wymiaru $v \times v$ jest więc macierzą incydencji konfiguracji kwadratowej o parametrach v, k, λ ($k < v-1$, $\lambda > 0$) wtedy i tylko wtedy, gdy spełnia równanie (2.6) lub równoważne mu równanie $AA^T = (k-\lambda)I+\lambda J$.

Pokażemy teraz jak z konfiguracji kwadratowej $\langle X, \mathscr{B}\rangle$ o parametrach v, k, λ, r, b można otrzymać dwie inne konfiguracje, już nie kwadratowe. W tym celu ustalmy pewien blok $B \in \mathscr{B}$. Niech $\mathscr{B}'$ będzie rodziną złożoną z przecięć tego bloku z pozostałymi blokami, tzn. $\mathscr{B}' = (B \cap C\colon C \in \mathscr{B} \setminus \{B\})$. Na mocy twierdzenia 2.1 $\langle B, \mathscr{B}'\rangle$ jest konfiguracją o parametrach

(2.8) $$v' = k, \quad k' = \lambda, \quad \lambda' = \lambda - 1, \quad r' = r-1, \quad b' = b-1,$$

jeśli tylko $1 < \lambda < k-1$, tak by spełniony był dla $\langle B, \mathscr{B}'\rangle$ warunek K4*. Nazywamy ją *konfiguracją pochodną*. Podobnie, para $\langle X \setminus B, \mathscr{B}^*\rangle$, gdzie $\mathscr{B}^* = (C \setminus B\colon C \in \mathscr{B} \setminus \{B\})$, jest konfiguracją o parametrach

(2.9) $$v^* = v-k, \quad k^* = k-\lambda, \quad \lambda^* = \lambda, \quad r^* = r, \quad b^* = b-1,$$

zwaną *konfigurację resztową* (należy tylko założyć $2k-\lambda+1 < v$).

Podamy przy okazji jeszcze jedną prostą konstrukcję, która stosuje się do dowolnych konfiguracji, niekoniecznie kwadratowych. Jeśli mianowicie w konfiguracji $\langle X, \mathscr{B}\rangle$ o parametrach v, k, λ, r, b, zastąpimy każdy blok B przez jego dopełnienie $X \setminus B$, to otrzymamy konfigurację o parametrach

(2.10) $$\bar{v} = v, \quad \bar{k} = v-k, \quad \bar{\lambda} = b-2r+\lambda, \quad \bar{r} = b-r, \quad \bar{b} = b,$$

zwaną *konfiguracją dopełnieniową* względem $\langle X, \mathscr{B}\rangle$. Aby sprawdzić, że tak jest w istocie, rozważmy podmacierz złożoną z dowolnych dwóch wierszy macierzy incydencji konfiguracji $\langle X, \mathscr{B}\rangle$. Podmacierz ta zawiera λ kolumn $\begin{bmatrix}1\\1\end{bmatrix}$, $r-\lambda$ kolumn $\begin{bmatrix}0\\1\end{bmatrix}$, $r-\lambda$ kolumn $\begin{bmatrix}1\\0\end{bmatrix}$, i w konsekwencji $b-\lambda-(r-\lambda)-(r-\lambda) = b-2r+\lambda$ kolumn $\begin{bmatrix}0\\0\end{bmatrix}$, które przechodzą na $\begin{bmatrix}1\\1\end{bmatrix}$ w konfiguracji dopełnieniowej.

Konfiguracje kwadratowe o $\lambda = 1$ wiążą się ściśle ze skończonymi płaszczyznami rzutowymi. Przypomnijmy (p. rozdział 1, § 12), że skończoną płaszczyzną rzutową o zbiorze punktów X i zbiorze prostych $\mathscr{B}$ nazywamy parę $\langle X, \mathscr{B}\rangle$, gdzie X jest zbiorem skończonym, $\mathscr{B}$ rodziną jego podzbiorów, oraz

---

* W przypadku, gdy warunek K4 nie jest spełniony, lecz każdy punkt występuje w takiej samej liczbie bloków, mówimy o tzw. *konfiguracji zdegenerowanej*.

PR1. Przez każde dwa różne punkty przechodzi dokładnie jedna prosta.

PR2. Każde dwie różne proste przechodzą przez dokładnie jeden wspólny punkt.

PR3. Istnieją cztery różne punkty, z których żadne trzy nie leżą na jednej prostej.

TWIERDZENIE 2.3. *Para $\langle X, \mathscr{B}\rangle$ jest skończoną płaszczyzną rzutową wtedy i tylko wtedy, gdy jest konfiguracją kwadratową z $\lambda = 1$.*

Dowód. Załóżmy, że $\langle X, \mathscr{B}\rangle$ jest konfiguracją kwadratową i $\lambda = 1$. Na mocy K3 jest wtedy spełniony warunek PR1 oraz – wobec twierdzenia 2.1 – warunek PR2. Wykażemy teraz, że zachodzi też warunek PR3. Istotnie, z (1.1) i K4 wynika, że $k < k(k-1)$, czyli $k \geqslant 3$. Rozważmy dowolne dwa bloki B_1, $B_2 \in \mathscr{B}$. Niech $B_1 \cap B_2 = \{p\}$. Istnieją wtedy dwa punkty $x, y \in B_1 \setminus \{p\}$ i dwa punkty z, $t \in B_2 \setminus \{p\}$. Łatwo widać, że punkty x, y, z, t mają własność, o której mowa w PR3.

Załóżmy teraz, że $\langle X, \mathscr{B}\rangle$ jest skończoną płaszczyzną rzutową. Wykażemy, że $\langle X, \mathscr{B}\rangle$ jest konfiguracją kwadratową o parametrze $\lambda = 1$. Na mocy lematu 12.5 z rozdziału 1 istnieje liczba k taka, że każda prosta liczy dokładnie k punktów, spełniony jest więc warunek KK1. Warunek KK2 to nic innego jak PR1. Spełniony jest również warunek KK3, gdyż żadna prosta nie zawiera co najmniej dwóch spośród czterech punktów, o których mowa w PR3. Tak więc $\langle X, \mathscr{B}\rangle$ jest konfiguracją kwadratową o parametrze $\lambda = 1$. □

Przypomnijmy, że liczbę $n = k-1$, gdzie k jest licznością każdej z prostych, nazywamy rzędem płaszczyzny rzutowej.

Z twierdzenia 2.2 i równości $\lambda(v-1) = k(k-1)$ (p. (2.1)) wynika, że $v = k(k-1)+1 = (n+1)n+1 = n^2+n+1$. Odnotujmy poznane elementarne zależności pomiędzy liczbą punktów i prostych płaszczyzny rzutowej (por. rozdz. 1, lemat 12.7).

TWIERDZENIE 2.4. *W dowolnej płaszczyźnie rzutowej rzędu n*

(a) *każda prosta zawiera $n+1$ punktów,*

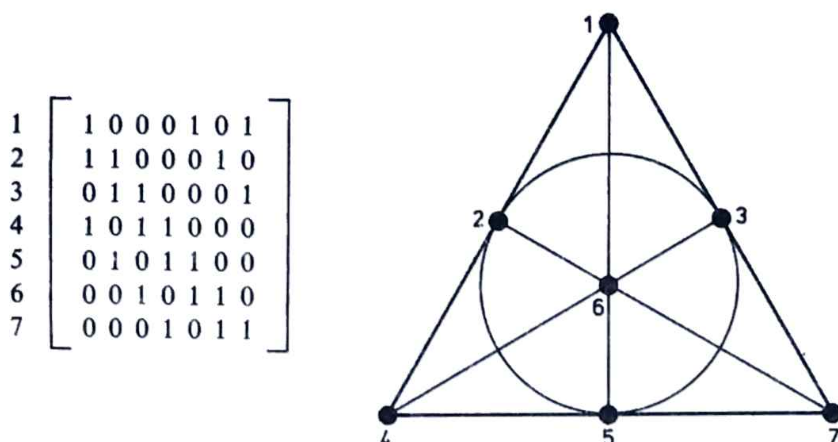
(b) *przez każdy punkt przechodzi $n+1$ prostych,*

(c) *wszystkich punktów jest n^2+n+1,*

(d) *wszystkich prostych jest n^2+n+1.*

W dowodzie twierdzenia 2.3 wykazaliśmy, że musi być $k > 2$, wartość $n = 1$ została więc wyeliminowana jako rząd płaszczyzny rzutowej (odpowiada jej „zdegenerowana płaszczyzna" o punktach a, b, c i prostych $\{a, b\}$, $\{b, c\}$, $\{a, c\}$, nie spełniająca warunku PR3).

Przypomnijmy, że z płaszczyznami rzutowymi pewnego szczególnego typu – mianowicie płaszczyznami $PG(2, n)$ – spotkaliśmy się już w rozdziale 1 (§ 12). Warto zauważyć, że konfiguracji o parametrach $v = 7$, $k = 3$, $\lambda = 1$ z przykładu (a) w § 1 odpowiada płaszczyzna Fano $PG(2, 2)$ (por. rys. 15). Ilustruje to rys. 29.



Rys. 29. Odpowiedniość między konfiguracją o parametrach $v=7$, $k=3$, $\lambda=1$ a płaszczyzną Fano

W § 4 przekonamy się, że nie dla każdego $n>1$ istnieje płaszczyzna rzutowa rzędu n. Z drugiej strony, dla n będącego potęgą liczby pierwszej płaszczyzna rzutowa zawsze istnieje – jest nią $PG(2, n)$ (p. rozdział 1, § 12; do zagadnienia tego wrócimy jeszcze w §§ 6 i 9). Choć znane są płaszczyzny rzutowe różne od $PG(2, n)$, to jednak rząd każdej takiej płaszczyzny jest potęgą liczby pierwszej. Niestety, w stosunku do pewnych wartości n nie wiadomo, czy są one rzędem płaszczyzny rzutowej. Pierwszą taką wartością jest już $n=10$. Tak więc nie wiadomo, czy istnieje macierz zero-jedynkowa A wymiaru 111×111 o 11 jedynkach w każdej kolumnie i wierszu, o iloczynie skalarnym dowolnych dwu wierszy równym jedności. Problemu tego, który teoretycznie daje się oczywiście rozstrzygnąć przez pełny przegląd skończonej liczby przypadków, nie udało się dotychczas rozwiązać nawet przy użyciu najszybszych dostępnych obecnie komputerów.

Na zakończenie tego paragrafu zauważmy, że z faktu, iż skończone płaszczyzny rzutowe są równoważne pewnym konfiguracjom kwadratowym oraz z twierdzenia 2.1 wynika następująca *zasada dualności*: Jeśli pewne zdanie P jest prawdziwe w dowolnej płaszczyźnie rzutowej, to zdanie dualne P^* powstałe z P przez zamianę rolami punktów i prostych (oraz relacji „leżenia na prostej" i „przechodzenia przez punkt") jest też prawdziwe w dowolnej płaszczyźnie rzutowej. Istotnie, jeśli $\langle X, \mathscr{B}\rangle$ jest płaszczyzną o macierzy incydencji A, to A^T jest macierzą incydencji płaszczyzny dualnej $\langle \mathscr{B}, X^*\rangle$, gdzie $X^* = (\{L \in \mathscr{B}\colon x \in L\}\colon x \in X)$. W płaszczyźnie dualnej rolę punktów przejmują więc proste płaszczyzny $\langle X, \mathscr{B}\rangle$, każda zaś prosta odpowiada pewnemu punktowi płaszczyzny $\langle X, \mathscr{B}\rangle$: jest ona zbiorem prostych płaszczyzny $\langle X, \mathscr{B}\rangle$ przechodzących przez ten punkt. Łatwo zauważyć, że zdanie P jest prawdziwe w $\langle X, \mathscr{B}\rangle$ wtedy i tylko wtedy, gdy zdanie P^* jest prawdziwe w $\langle \mathscr{B}, X^*\rangle$. Stąd łatwo już wynika zasada dualności, wystarczy jedynie zauważyć, że każda płaszczyzna $\langle X, \mathscr{B}\rangle$ jest (izomorficzna z) płaszczyzną dualną do pewnej płaszczyzny, mianowicie do płaszczyzny $\langle \mathscr{B}, X^*\rangle$. Z zasady dualności wynika, między innymi, że do aksjomatów PR1, PR2, PR3 możemy dodać jeszcze jeden:

PR3*. Istnieją cztery różne proste, z których żadne trzy nie przechodzą przez jeden punkt.

Otrzymujemy w ten sposób układ, w którym rola punktów i prostych jest w pełni symetryczna (zauważmy, że PR1* = PR2, PR2* = PR1).

§ 3. λ-konfiguracje

W poprzednim paragrafie pokazaliśmy, że konfigurację kwadratową $\langle X, \mathscr{B}\rangle$, $\mathscr{B} = (B_1, \ldots, B_v)$, można w pełni scharakteryzować przez następujące trzy warunki:

KK1. $|B_i| = k$ dla $1 \leqslant i \leqslant v$.

KK2. $|B_i \cap B_j| = \lambda$ dla $1 \leqslant i < j \leqslant v$.

KK3. $\lambda > 0$ oraz $k < v-1$.

Okazuje się, że sytuacja, w której nie żądamy spełnienia warunku KK1, jest niemniej ciekawa. Przez *λ-konfigurację* na zbiorze v-elementowym X będziemy rozumieli rodzinę $(B_1, \ldots, B_v)$ podzbiorów zbioru X spełniającą warunki

Λ1. $|B_i| = k_i > \lambda$ dla $1 \leqslant i \leqslant v$.

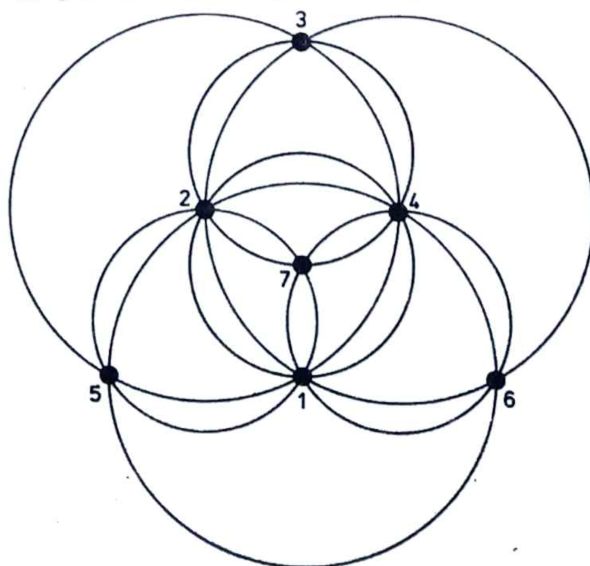
Λ2. $|B_i \cap B_j| = \lambda$ dla $1 \leqslant i < j \leqslant v$.

Λ3. $v > 3$ oraz nie wszystkie liczby k_i są równe.

Podamy teraz przykład λ-konfiguracji o parametrze $\lambda = 2$, tzn. 2-konfiguracji, na zbiorze $\{1, \ldots, 7\}$ (pochodzi on od de Witte'a [1]). Jako bloki przyjmujemy zbiory

$$\{1, 2, 4\},$$
$$\{1, 2, 6, 7\}, \quad \{2, 5, 7, 1\}, \quad \{3, 6, 1, 2\},$$
$$\{4, 7, 2, 3\}, \quad \{5, 1, 3, 4\}, \quad \{6, 2, 4, 5\}.$$

Mamy $v = 7$, $k_1 = 3$, $k_2 = \ldots = k_7 = 4$. Konfiguracja ta ma bardzo ciekawą reprezentację graficzną, pokazaną na rys. 30. Rysunek ten składa się z siedmiu



Rys. 30. 2-konfiguracja na zbiorze $\{1, \ldots, 7\}$.

okręgów (czterech mniejszych i trzech większych), które przecinają się w siedmiu punktach oznaczonych przez 1, ..., 7. Każdy blok odpowiada zbiorowi punktów przecięć na pewnym okręgu.

Z definicji λ-konfiguracji wynika, że jej macierz incydencji spełnia równanie

$$A^T A = \operatorname{diag}[k_1 - \lambda, \ldots, k_v - \lambda] + \lambda J, \tag{3.1}$$

gdzie $\operatorname{diag}[k_1 - \lambda, \ldots, k_v - \lambda]$ oznacza macierz o elementach $k_1 - \lambda, \ldots, k_v - \lambda$ na głównej przekątnej i 0 w pozostałych pozycjach, J zaś macierz złożoną z samych jedynek. Udowodnimy najpierw pewne uogólnienie nierówności Fishera.

TWIERDZENIE 3.1 (Majumdar [1]). *Niech A będzie macierzą zero-jedynkową o m wierszach i n kolumnach spełniającą równanie*

$$A^T A = \operatorname{diag}[k_1 - \lambda, \ldots, k_n - \lambda] + \lambda J,$$

gdzie $\lambda \geqslant 1$, $n > 1$ oraz $k_i > \lambda$ dla $1 \leqslant i \leqslant n$. Wówczas $m \geqslant n$.

Dowód. Wykażemy najpierw, że $\det(A^T A) \neq 0$. Postępujemy podobnie jak w dowodzie lematu 1.2. Odejmujemy pierwszą kolumnę macierzy $A^T A$ od pozostałych. Następnie, dla $i = 2, \ldots, n$, dodajemy do pierwszego wiersza powstałej macierzy wiersz i-ty pomnożony przez $(k_1 - \lambda)/(k_i - \lambda)$. Otrzymujemy macierz, która ma same zera ponad główną przekątną oraz wartości

$$k_1 + \lambda(k_1 - \lambda)\left(\frac{1}{k_2 - \lambda} + \ldots + \frac{1}{k_n - \lambda}\right), \quad k_2 - \lambda, \quad \ldots, \quad k_n - \lambda$$

na przekątnej. Stąd

$$\det(A^T A) = \left[k_1 + \lambda(k_1 - \lambda)\left(\frac{1}{k_2 - \lambda} + \ldots + \frac{1}{k_n - \lambda}\right)\right](k_2 - \lambda) \ldots (k_n - \lambda) =$$

$$= \left[1 + \lambda\left(\frac{1}{k_1 - \lambda} + \ldots + \frac{1}{k_n - \lambda}\right)\right](k_1 - \lambda) \ldots (k_n - \lambda) \neq 0.$$

Dalej dowód przebiega identycznie jak dowód twierdzenia 1.3. □

Zauważmy, że istota tego twierdzenia, jak również nierówność Fishera, jest następująca: Jeśli $S_1, \ldots, S_n$ są podzbiorami zbioru m-elementowego takimi, że każde dwa zbiory mają dokładnie λ elementów wspólnych, to — przy odpowiednich założeniach eliminujących przypadki zdegenerowane — musi być $m \geqslant n$. W przypadku nierówności Fishera zakładaliśmy, że wszystkie zbiory są jednakowej liczności (równej r), teraz żądamy jedynie, by żaden ze zbiorów nie zawierał się w innym. Tak więc zarówno konfiguracje kwadratowe jak i λ-konfiguracje są przypadkiem granicznym odpowiadającym równości $m = n$. Jednym z najciekawszych wyników dotyczących λ-konfiguracji jest następujące twierdzenie podane niezależnie przez Rysera [3] i Woodalla [1]. Zanim je sformułujemy wprowadzimy

następujące oznaczenia dotyczące λ-konfiguracji o parametrach $v, k_1, \ldots, k_v$ i macierzy incydencji $A = [a_{ij}]$:

$$R = \frac{1}{\lambda} + \sum_{m=1}^{v} \frac{1}{k_m - \lambda}, \tag{3.2}$$

$$R_{ij} = \sum_{m=1}^{v} \frac{a_{im} a_{jm}}{k_m - \lambda}, \tag{3.3}$$

$$R_i = R_{ii} = \sum_{m=1}^{v} \frac{a_{im}}{k_m - \lambda}, \tag{3.4}$$

$$P = \prod_{m=1}^{v} (k_m - \lambda). \tag{3.5}$$

Zauważmy, że przy tych oznaczeniach $\det(A^T A) = \lambda R P$.

TWIERDZENIE 3.2. *Niech $a = [a_{ij}]$ będzie macierzą incydencji λ-konfiguracji na zbiorze v-elementowym. Wówczas suma elementów w wierszu macierzy A przyjmuje dokładnie dwie różne wartości r_1 i r_2, przy czym*

$$r_1 + r_2 = v + 1. \tag{3.6}$$

Dowód. Utwórzmy dla $i = 1, 2, \ldots, v$ macierz C_i przez dodanie do A najpierw $(v+1)$-szej kolumny mającej jedynkę w wierszu i-tym i zera w pozostałych, a następnie $(v+1)$-szego wiersza złożonego z samych zer. Oczywiście $\det C_i = 0$, a więc również

$$\det(C_i^T C_j) = \begin{vmatrix} k_1 & \lambda & \ldots & \lambda & a_{j1} \\ \lambda & k_2 & & \lambda & a_{j2} \\ \vdots & & \ddots & & \vdots \\ \lambda & \lambda & \ldots & k_v & a_{jv} \\ a_{i1} & a_{i2} & \ldots & a_{iv} & \delta_{ij} \end{vmatrix} = 0 \tag{3.7}$$

dla $1 \leqslant i, j \leqslant v$ (δ_{ij} oznacza deltę Kroneckera: $\delta_{ii} = 1$, $\delta_{ij} = 0$ dla $i \neq j$). Obliczymy teraz wyznacznik po prawej stronie (3.7).

Najpierw odejmujemy pierwszą kolumnę od wszystkich pozostałych z wyjątkiem ostatniej. Następnię dla $m = 2, 3, \ldots, v$, dodajemy m-ty wiersz pomnożony przez $(k_1 - \lambda)/(k_m - \lambda)$ do pierwszego wiersza. Otrzymujemy w ten sposób następujący wyznacznik

$$\begin{vmatrix} \lambda(k_1-\lambda)R & 0 & 0 & \ldots & 0 & (k_1-\lambda)R_j \\ \lambda & k_2-\lambda & 0 & & 0 & a_{j2} \\ \lambda & 0 & k_3-\lambda & & 0 & a_{j3} \\ \vdots & & & \ddots & & \vdots \\ \lambda & 0 & 0 & & k_v-\lambda & a_{jv} \\ a_{i1} & a_{i2}-a_{i1} & a_{i3}-a_{i1} & \ldots & a_{iv}-a_{i1} & \delta_{ij} \end{vmatrix}.$$

Element w lewym górnym rogu otrzymujemy na podstawie następujących przekształceń:

$$k_1+\sum_{m=2}^{v}\frac{\lambda(k_1-\lambda)}{k_m-\lambda}=(k_1-\lambda)+\lambda+\sum_{m=2}^{v}\frac{\lambda(k_1-\lambda)}{(k_m-\lambda)}=$$
$$=(k_1-\lambda)\lambda\left[\frac{1}{\lambda}+\frac{1}{k_1-\lambda}+\sum_{m=2}^{v}\frac{1}{k_m-\lambda}\right]=(k_1-\lambda)\lambda R,$$

natomiast element w prawym górnym rogu obliczamy następująco:

$$a_{j1}+\sum_{m=2}^{v}\frac{(k_1-\lambda)a_{jm}}{k_m-\lambda}=(k_1-\lambda)\left[\frac{a_{j1}}{k_1-\lambda}+\sum_{m=2}^{v}\frac{a_{jm}}{k_m-\lambda}\right]=(k_1-\lambda)R_j.$$

Odejmujemy teraz m-tą kolumnę pomnożoną przez $\lambda/(k_m-\lambda)$ od pierwszej kolumny, oraz pomnożoną przez $a_{jm}/(k_m-\lambda)$ od $(v+1)$-szej kolumny dla $m=2,3,\ldots,v$, a następnie odejmujemy pierwszy wiersz pomnożony przez $a_{i1}/(k_1-\lambda)$ od ostatniego wiersza. Otrzymujemy wyznacznik

$$\begin{vmatrix}\lambda(k_1-\lambda)R & 0 & 0 & \ldots & 0 & (k_1-\lambda)R_j\\ 0 & k_2-\lambda & 0 & & 0 & 0\\ 0 & 0 & k_3-\lambda & & 0 & 0\\ \vdots & & & \ddots & & \vdots\\ 0 & 0 & 0 & \ldots & k_v-\lambda & 0\\ -\lambda R_i & a_{i2}-a_{i1} & a_{i3}-a_{i1} & & a_{iv}-a_{i1} & \delta_{ij}-R_{ij}\end{vmatrix}.$$

Element w lewym dolnym rogu obliczamy w następujący sposób:

$$a_{i1}-\sum_{m=2}^{v}\frac{(a_{im}-a_{i1})\lambda}{k_m-\lambda}-\lambda a_{i1}R=a_{i1}\lambda\left[\frac{1}{\lambda}+\sum_{m=2}^{v}\frac{1}{k_m-\lambda}-R\right]-\lambda\sum_{m=2}^{v}\frac{a_{im}}{k_m-\lambda}=$$
$$=\lambda\left(a_{i1}\frac{-1}{k_1-\lambda}-\sum_{m=2}^{v}\frac{a_{im}}{k_m-\lambda}\right)=-\lambda R_i,$$

a w prawym dolnym –

$$\delta_{ij}-\sum_{m=2}^{v}\frac{(a_{im}-a_{i1})a_{jm}}{k_m-\lambda}-a_{i1}R_j=\delta_{ij}-\sum_{m=2}^{v}\frac{a_{im}a_{jm}}{k_m-\lambda}+a_{i1}\left(\sum_{m=2}^{v}\frac{a_{jm}}{k_m-\lambda}-R_j\right)=\delta_{ij}-R_{ij}.$$

Teraz łatwo już widać, że nasz wyznacznik jest równy

$$\lambda P\begin{vmatrix}R & R_j\\ -R_i & \delta_{ij}-R_{ij}\end{vmatrix}=\lambda P[R(\delta_{ij}-R_{ij})+R_iR_j].$$

Równanie (3.7) przyjmuje zatem postać

$$R(\delta_{ij}-R_{ij})+R_iR_j=0, \tag{3.8}$$

czyli

(3.9) $$R_i^2 - RR_i + R = 0$$

dla $i = j$, oraz

(3.10) $$R_{ij} = \frac{R_i R_j}{R}$$

dla $i \neq j$. Skoro liczby R_i spełniają równanie kwadratowe (3.9), to mogą one przyjmować najwyżej dwie wartości — oznaczmy je przez S_1 i S_2. Mamy

(3.11) $$\sum_{j=1}^{v} R_j = \sum_{j=1}^{v} \sum_{m=1}^{v} \frac{a_{jm}}{k_m - \lambda} = \sum_{m=1}^{v} \frac{k_m}{k_m - \lambda} = \sum_{m=1}^{v} \left(1 + \frac{\lambda}{k_m - \lambda}\right) = v + \lambda\left(R - \frac{1}{\lambda}\right) = v - 1 + \lambda R,$$

(3.12) $$\sum_{j=1}^{v} R_{ij} = \sum_{j=1}^{v} \sum_{m=1}^{v} \frac{a_{im} a_{jm}}{k_m - \lambda} = \sum_{m=1}^{v} \frac{a_{im} k_m}{k_m - \lambda} = \sum_{m=1}^{v} \left(a_{im} + \frac{a_{im}\lambda}{k_m - \lambda}\right) = s_i + \lambda R_i,$$

gdzie s_i oznacza sumę i-tego wiersza macierzy A. Sumując stronami równania (3.8) dla $j = 1, 2, \ldots, v$ i korzystając z (3.11) i (3.12) otrzymujemy

$$R - R(s_i + \lambda R_i) + R_i(v - 1 + \lambda R) = 0,$$

a stąd

(3.13) $$s_i = \frac{(v-1)R_i}{R} + 1.$$

Zatem s_i może przyjmować również tylko dwie wartości, mianowicie

(3.14) $$r_1 = \frac{(v-1)S_1}{R} + 1, \quad r_2 = \frac{(v-1)S_2}{R} + 1.$$

Oczywiście musi być $r_1 \neq r_2$, gdyż w przeciwnym razie A^T byłaby macierzą incydencji konfiguracji kwadratowej (być może zdegenerowanej), tzn. byłoby $k_1 = \ldots = k_v$, wbrew warunkowi $\Lambda 3$. W myśl wzorów Viète'a dla pierwiastków S_1, S_2 równania (3.9) mamy

(3.15) $$S_1 + S_2 = S_1 S_2 = R.$$

A zatem

$$r_1 + r_2 = \frac{(v-1)(S_1 + S_2)}{R} + 2 = v + 1. \quad \square$$

Aby bliżej poznać strukturę λ-konfiguracji, wprowadzimy teraz pewne dodatkowe zależności między jej parametrami. Przyjmujemy umowę, że $r_1 > r_2$, oraz że

macierz incydencji λ-konfiguracji jest zawsze doprowadzona do postaci

$$A = \begin{bmatrix} A_1 \\ \cdots\cdots \\ A_2 \end{bmatrix},$$

gdzie A_1 składa się z wierszy o sumie r_1, A_2 zaś z wierszy o sumie r_2. Oznaczmy liczbę wierszy macierzy A_1 i A_2 odpowiednio przez e_1 i e_2, oraz sumę elementów j-tej kolumny macierzy A_1 i A_2 odpowiednio przez k'_j i k^*_j. Oczywiście

$$k_j = k'_j + k^*_j.$$

Obliczając na dwa sposoby sumę iloczynów skalarnych j-tej kolumny macierzy A przez wszystkie pozostałe kolumny, otrzymujemy równość

$$\lambda(v-1) = \sum_{m\neq j}\sum_{i=1}^{v} a_{im}a_{ij} = \sum_{i=1}^{v}(s_i - a_{ij})a_{ij} = \tag{3.16}$$
$$= k'_j(r_1-1) + k^*_j(r_2-1).$$

Oczywiście $R > 0$, a więc na mocy wzoru (3.15) liczby S_1, S_2 są dodatnie i wobec (3.14) mamy $r_1, r_2 > 1$, czyli

$$r_1 \geqslant 3, \qquad r_2 \geqslant 2. \tag{3.17}$$

Możemy zatem wprowadzić oznaczenie

$$\varrho = \frac{r_1-1}{r_2-1} > 1. \tag{3.18}$$

Uwzględniając zależność $(r_1-1)+(r_2-1) = v-1$ możemy parametry r_1, r_2 przedstawić jako

$$r_1 = \frac{v\varrho+1}{\varrho+1}, \qquad r_2 = \frac{\varrho+v}{\varrho+1}. \tag{3.19}$$

Sumując równania (3.16) dla $j = 1, 2, \ldots, v$ otrzymujemy

$$\lambda v(v-1) = e_1 r_1(r_1-1) + e_2 r_2(r_2-1). \tag{3.20}$$

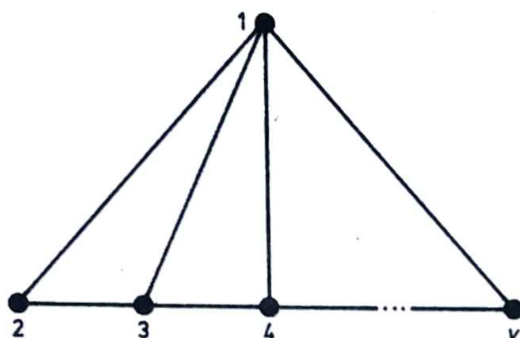
Stąd po podzieleniu stronami przez r_2-1, skorzystaniu z zależności (3.19) oraz uwzględnieniu równości $e_2 = v - e_1$ otrzymujemy

$$e_1 = \frac{\lambda(\varrho+1)^2 - (\varrho+v)}{\varrho^2-1}. \tag{3.21}$$

Zajmiemy się teraz bliżej przypadkiem $\lambda = 1$. Okazuje się, że możemy dokładnie opisać postać 1-konfiguracji na zbiorze v-elementowym.

TWIERDZENIE 3.3 (de Bruijn i Erdős [1]). *Jedyną (z dokładnością do izomorfizmu) 1-konfiguracją na zbiorze* $\{1, \ldots, v\}$, $v > 3$, *jest 1-konfiguracja o blokach*

$B_1 = \{2, 3, \ldots, v\}$, $B_2 = \{1, 2\}$, $B_3 = \{1, 3\}, \ldots, B_v = \{1, v\}$ *przedstawiona graficznie na rys* 31.



Rys. 31. Przedstawienie graficzne 1-konfiguracji na zbiorze $1, \ldots, v$

Dowód. Zauważmy przede wszystkim, że $2r_1 \geqslant r_1 + r_2 + 1 = v + 2$. Musi więc być $e_1 = 1$ — w przeciwnym razie macierz incydencji A naszej konfiguracji musiałaby zawierać dwie kolumny o iloczynie skalarnym równym co najmniej 2. Podstawiając $\lambda = e_1 = 1$ do wzoru (3.21) otrzymujemy $\varrho = v - 2$. Na mocy zależności (3.19) $r_1 = v - 1$ oraz $r_2 = 2$. Łatwo się teraz przekonać, że macierz incydencji naszej 1-konfiguracji ma — po ewentualnym dokonaniu permutacji wierszy i kolumn — postać

$$A = \begin{bmatrix} 0 & 1 & 1 & \ldots & 1 \\ 1 & 1 & 0 & & 0 \\ 1 & 0 & 1 & & 0 \\ \vdots & & & \ddots & \\ 1 & 0 & 0 & & 1 \end{bmatrix}. \tag{3.22}$$

Lecz jest to właśnie macierz incydencji 1-konfiguracji, o której mowa w tezie twierdzenia. □

Warto przy okazji zauważyć, że 1-konfiguracje spełniają aksjomaty PR1 i PR2 płaszczyzny rzutowej. Zatem warunek PR3 wyklucza znacznie więcej niż tylko zdegenerowaną płaszczyznę rzutową o trzech punktach.

Przy przejściu od $\lambda = 1$ do przypadku $\lambda > 1$ sytuacja znacznie się zmienia. Wykażemy mianowicie, że dla każdego $\lambda > 1$ liczba nieizomorficznych λ-konfiguracji jest skończona. Udowodnimy najpierw następujący lemat.

LEMAT 3.4. *Równość $e_1 = 1$ zachodzi tylko dla 1-konfiguracji.*

Dowód. Rozważmy dowolną λ-konfigurację, dla której $e_1 = 1$. Jej macierz incydencji możemy — po ewentualnej permutacji wierszy i kolumn — przedstawić w postaci

$$A = \left[\begin{array}{c:c} 1 \ldots 1 & 0 \ldots 0 \\ \hdashline B & C \end{array}\right],$$

gdzie B i C są macierzami wymiaru odpowiednio $(v-1)\times r_1$ i $(v-1)\times(v-r_1)$. Równanie (3.16) po podzieleniu stronami przez r_2-1 i elementarnych przekształceniach przyjmuje postać

$$k_j^* = \lambda(\varrho+1)-\varrho k_j'. \tag{3.23}$$

Mamy $k_j'=1$ dla $1\leqslant j\leqslant r_1$ oraz $k_j'=0$ dla $r_1+1\leqslant j\leqslant v$. A zatem

$$k_j = \lambda(\varrho+1)-\varrho+1 \quad \text{dla } 1\leqslant j\leqslant r_1 \tag{3.24}$$

oraz

$$k_j = \lambda(\varrho+1) \quad \text{dla } r_1+1\leqslant j\leqslant v. \tag{3.25}$$

Dla $2\leqslant j\leqslant v$

$$R_{1j} = \sum_{m=1}^{v}\frac{a_{1m}a_{jm}}{k_m-\lambda} = \frac{1}{\lambda\varrho-\varrho+1}\sum_{m=1}^{r_1} a_{jm}.$$

Lecz na mocy wzorów (3.10) i (3.15)

$$R_{1j} = \frac{R_1R_j}{R} = \frac{S_1S_2}{R} = 1,$$

gdyż wobec (3.13) $R_j\neq R_1$ dla $2\leqslant j\leqslant v$.

Suma każdego wiersza macierzy B jest więc stała i wynosi

$$\sum_{m=1}^{r_1} a_{jm} = \lambda\varrho-\varrho+1.$$

Zatem stała jest również suma każdego wiersza macierzy C. Licząc jedynki w macierzy C na dwa sposoby łatwo się przekonać, że suma ta jest równa

$$\frac{\lambda(\varrho+1)(v-r_1)}{v-1} = \frac{\lambda(v-1)(r_2-1)}{(r_2-1)(v-1)} = \lambda.$$

Obliczmy teraz R_{ij} dla $2\leqslant i<j\leqslant v$. Na mocy wzorów (3.10), (3.15) i (3.14)

$$R_{ij} = \frac{R_iR_j}{R} = \frac{S_2S_2}{S_1S_2} = \frac{S_2}{S_1} = \frac{r_2-1}{r_1-1} = \frac{1}{\varrho}. \tag{3.26}$$

Z drugiej strony, oznaczając, dla ustalonych i, j,

$$b = \sum_{m=1}^{r_1} a_{im}a_{jm}, \quad c = \sum_{m=r_1+1}^{v} a_{im}a_{jm}$$

mamy

$$R_{ij} = \frac{b}{\lambda\varrho-\varrho+1}+\frac{c}{\lambda\varrho}.$$

Porównując to wyrażenie z (3.26) otrzymujemy równanie

(3.27) $$\frac{b}{\lambda\varrho-\varrho+1}+\frac{c}{\lambda\varrho}=\frac{1}{\varrho},$$

które możemy zapisać jako

(3.28) $$\lambda\varrho(b+c)=\lambda^2\varrho-(\varrho-1)(c-\lambda).$$

Załóżmy, że $c<\lambda$. Wówczas z (3.28) otrzymujemy

(3.29) $$b+c<\lambda.$$

Równanie (3.28) możemy przekształcić do postaci

$$\varrho[\lambda^2-\lambda(b+c+1)+c]=c-\lambda<0.$$

Stąd, biorąc pod uwagę (3.29), otrzymujemy

$$\lambda^2+c<\lambda(b+c+1)\leqslant\lambda^2.$$

Sprzeczność ta dowodzi, że parametr c obliczony dla dowolnych $2\leqslant i<j\leqslant v$ musi być równy λ. Oznacza to, że macierz C zawiera λ kolumn złożonych z samych jedynek. Musi więc być $\lambda=1$ – w przeciwnym razie dla tych kolumn mielibyśmy $k_j=\lambda$, wbrew warunkowi $\Lambda1$. □

LEMAT 3.5. *Jeśli $\lambda>1$, to dla dowolnej λ-konfiguracji $\varrho\leqslant\lambda$.*

Dowód. Jeśli $\lambda>1$, to na mocy poprzedniego lematu $e_1\geqslant 2$. Mamy zatem

$$0\leqslant\sum_{m=1}^{v}\frac{(1-a_{1m})(1-a_{2m})}{(k_m-\lambda)}=R-\frac{1}{\lambda}-R_1-R_2+R_{12}=$$
$$=R-2S_1+\frac{(R-S_2)(R-S_2)}{R}-\frac{1}{\lambda}=\frac{S_2S_2}{R}-\frac{1}{\lambda}.$$

Korzystając z (3.26) otrzymujemy

$$\frac{1}{\varrho}-\frac{1}{\lambda}=\frac{\lambda-\varrho}{\varrho\lambda}\geqslant 0.\ \square$$

TWIERDZENIE 3.6 (Woodall [1]). *Dla dowolnego $\lambda>1$ liczba nieizomorficznych λ-konfiguracji jest skończona.*

Dowód. Ze wzoru (3.21) i poprzednich lematów otrzymujemy

$$v=\lambda(\varrho+1)^2-e_1(\varrho^2-1)-\varrho\leqslant\lambda\varrho^2+2\lambda\varrho+\lambda-2\varrho^2+2-\varrho=$$
$$=(\lambda-2)\varrho^2+(2\lambda-1)\varrho+2\leqslant(\lambda-2)\lambda^2+(2\lambda-1)\lambda+2=$$
$$=\lambda^3-\lambda+2.$$

Twierdzenie wynika teraz z oczywistego faktu, iż dla ustalonego v istnieje tylko

skończona liczba nieizomorficznych λ-konfiguracji, na pewno mniejsza od 2^{v^2} – liczby wszystkich macierzy zero-jedynkowych wymiaru $v\times v$. □

Twierdzenie to jest o tyle ciekawe, że analogiczny problem dla konfiguracji kwadratowych jest nierozstrzygnięty.

Można pokazać, że jedyną 2-konfiguracją jest przedstawiona na rys. 30. Wszystkie nieizomorficzne λ-konfiguracje dla $\lambda = 3$ zostały wyznaczone przez Bridgesa i Kramera [1], oraz dla $4 \leqslant \lambda \leqslant 9$ przez Kramera [1].

Na zakończenie tego paragrafu podamy pewną ogólną metodę konstruowania λ-konfiguracji. Niech A będzie macierzą kwadratową zero-jedynkową wymiaru $v\times v$. Przez *uzupełnienie* A względem j-tej kolumny ($1 \leqslant j \leqslant v$) będziemy rozumieli macierz powstałą z A przez odjęcie j-tej kolumny od wszystkich pozostałych kolumn, a następnie zamianę elementów -1 na 1. Konfigurację będziemy utożsamiali z jej macierzą incydencji.

TWIERDZENIE 3.7. *Uzupełnienie względem j-tej kolumny*
(a) *konfiguracji kwadratowej o parametrach*

$$v = 4\lambda-1, \qquad k = 2\lambda, \qquad \lambda$$

jest konfiguracją kwadratową o tych samych parametrach,

(b) *konfiguracji kwadratowej (być może zdegenerowanej) o parametrach* v, k, λ, *gdzie* $k \neq 2\lambda$, *jest* $(k-\lambda)$-*konfiguracją,*

(c) λ-*konfiguracji jest albo* $(k_j-\lambda)$-*konfiguracją, albo konfiguracją kwadratową (być może zdegenerowaną) o parametrach* v, k_j, $k_j-\lambda$.

Dowód. Niech A będzie zero-jedynkową macierzą wymiaru $v\times v$ taką, że $A^TA = \mathrm{diag}[k_1-\lambda, \ldots, k_v-\lambda]+\lambda J$. Oznaczmy przez $\bar{A}$ uzupełnienie A względem j-tej kolumny. Wykażemy, że iloczyn skalarny dowolnych dwu kolumn macierzy $\bar{A}$ jest równy $k_j-\lambda$. Jeśli jedna z kolumn jest kolumną j-tą, to przez dokonanie odpowiedniej permutacji wierszy odpowiednie kolumny macierzy A można sprowadzić do postaci

$$\begin{array}{c} k_j\left\{\begin{array}{cc}1&1\\ \vdots&\vdots\\ 1&1\\ 1&0\\ \vdots&\vdots\\ 1&0\end{array}\right.\begin{array}{l}\left.\begin{array}{c}\\ \\ \\ \end{array}\right\}\lambda\\ \left.\begin{array}{c}\\ \\ \\ \end{array}\right\}k_j-\lambda\end{array}\\ \begin{array}{cc}0&1\\ \vdots&\vdots\\ 0&1\\ 0&0\\ \vdots&\vdots\\ 0&0\end{array}\end{array}$$

i iloczyn skalarny odpowiednich kolumn macierzy $\bar{A}$ jest równy $k_j-\lambda$. Jeśli żadna

z naszych kolumn nie jest kolumną j-tą, to kolumny te wraz z j-tą kolumną mają – z dokładnością do permutacji wierszy – postać

$$
\begin{array}{c}
k_j\left\{\begin{array}{c}
\left.\begin{array}{ccc}1&1&1\\ \vdots&\vdots&\vdots\\ 1&1&1\end{array}\right\}\sigma\\
\left.\begin{array}{ccc}1&1&0\\ \vdots&\vdots&\vdots\\ 1&1&0\end{array}\right\}\lambda-\sigma\\
\left.\begin{array}{ccc}1&0&1\\ \vdots&\vdots&\vdots\\ 1&0&1\end{array}\right\}\lambda-\sigma\\
\left.\begin{array}{ccc}1&0&0\\ \vdots&\vdots&\vdots\\ 1&0&0\end{array}\right\}k_j-2\lambda+\sigma
\end{array}\right.\\
\left.\begin{array}{ccc}0&1&1\\ \vdots&\vdots&\vdots\\ 0&1&1\end{array}\right\}\lambda-\sigma\\
\begin{array}{ccc}0&1&0\\ \vdots&\vdots&\vdots\\ 0&1&0\\ 0&0&1\\ \vdots&\vdots&\vdots\\ 0&0&1\\ 0&0&0\\ \vdots&\vdots&\vdots\\ 0&0&0\end{array}
\end{array}
\qquad \text{(grupy } k_j-2\lambda+\sigma \text{ i } \lambda-\sigma \text{ razem: } k_j-\lambda)
$$

i iloczyn skalarny naszych dwu kolumn macierzy $\bar{A}$ jest równy $k_j-2\lambda+\sigma+\lambda-\sigma=k_j-\lambda$. Otrzymujemy zatem równość

$$
\bar{A}^T\bar{A}=\operatorname{diag}[\bar{k}_1-(k_j-\lambda),\ \ldots,\ \bar{k}_{j-1}-(k_j-\lambda),\ k_j-(k_j-\lambda),\ \bar{k}_{j+1}-(k_j-\lambda),\ \ldots
$$
$$
\ldots,\ \bar{k}_v-(k_j-\lambda)]+(k_j-\lambda)J,
$$

gdzie $\bar{k}_i=k_i+k_j-2\lambda$ dla $i\neq j$. Macierz $\bar{A}$ określa więc albo $(k_j-\lambda)$-konfigurację, albo konfigurację kwadratową o parametrach v, k_j, $k_j-\lambda$, być może zdegenerowaną. Dowodzi to punktu (c). Jeśli $k_j=2\lambda$, to $k_j-\lambda=\lambda$ oraz $\bar{k}_i=k_i$. Stąd wynika punkt (a). W przypadku $k_j\neq 2\lambda$ mamy $\bar{k}_i\neq k_i$, co dowodzi punktu (b). □

Zauważmy, że każda 1-konfiguracja jest uzupełnieniem względem pierwszej kolumny następującej zdegenerowanej konfiguracji kwadratowej o parametrach v, $k=v-1$, $\lambda=v-2$:

$$
J-I=\begin{bmatrix}0&1&1&\ldots&1\\ 1&0&1&\ldots&1\\ 1&1&0&&1\\ \vdots&&&\ddots&\vdots\\ 1&1&1&\ldots&0\end{bmatrix}.
$$

Wszystkie znane obecnie λ-konfiguracje są uzupełnieniami pewnych konfiguracji kwadratowych. Daje to podstawę do hipotezy – dotychczas nierozstrzygniętej – że każda λ-konfiguracja jest uzupełnieniem pewnej konfiguracji kwadratowej (być może zdegenerowanej). Zostało to sprawdzone dla wspomnianego już zakresu $1 \leqslant \lambda \leqslant 9$ (p. Kramer [1]) oraz dla przypadku, gdy λ jest liczbą pierwszą (p. Singhi i Shrikhande [1]).

§ 4. Twierdzenie Brucka–Rysera–Chowli

Powracamy obecnie do teorii konfiguracji kwadratowych. W paragrafie tym wykażemy fundamentalne twierdzenie dotyczące istnienia takich konfiguracji. Zostało ono udowodnione najpierw dla przypadku $\lambda = 1$ (tzn. dla płaszczyzn rzutowych) przez Brucka i Rysera [1], a następnie w całej ogólności przez Chowlę i Rysera [1].

TWIERDZENIE 4.1 (Bruck, Ryser i Chowla). *Załóżmy, że istnieje konfiguracja kwadratowa o parametrach v, k, λ, $n = k-\lambda$. Wówczas*

(a) *jeśli v jest parzyste, to n jest kwadratem liczby całkowitej,*

(b) *jeśli v jest nieparzyste, to istnieją liczby całkowite x, y, z, nie wszystkie równe zeru, spełniające równanie*

$$z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2. \tag{4.1}$$

Dowód. Niech $A = [a_{ij}]$ będzie macierzą incydencji naszej konfiguracji kwadratowej.

(a) Na mocy lematu 1.2 oraz zależności $\lambda(v-1) = k(k-1)$ (p. (1.1)) mamy

$$\det(AA^T) = (k-\lambda)^{v-1}\big(k(k-1)+k\big) = n^{v-1}k^2.$$

Wobec równości $\det(AA^T) = (\det A)(\det A^T) = (\det A)^2$ wnioskujemy stąd, że n jest kwadratem liczby całkowitej, mianowicie

$$n = \frac{(\det A)^2}{n^{v-2}k^2} = \left(\frac{\det A}{n^{v/2-1}k}\right)^2.$$

Korzystamy tu z elementarnego faktu, że dla dowolnych liczb całkowitych a, b mamy $a^2|b^2 \Leftrightarrow a|b$.

(b) Dowód tego przypadku jest nieco trudniejszy. Rozważmy formy liniowe

$$L_j = \sum_{i=1}^{v} a_{ij}x_i, \qquad 1 \leqslant j \leqslant v.$$

Korzystając z zależności $AA^T = (k-\lambda)I + \lambda J$ otrzymujemy następującą równość form kwadratowych:

$$L_1^2 + \ldots L_v^2 = \sum_{j=1}^{v}\sum_{p=1}^{v} a_{pj}x_p \sum_{q=1}^{v} a_{qj}x_q = \tag{4.2}$$

$$= \sum_{j=1}^{v} \sum_{p=1}^{v} \sum_{q=1}^{v} a_{pj} a_{qj} x_p x_q =$$
$$= \sum_{p=1}^{v} \sum_{q=1}^{v} \sum_{j=1}^{v} a_{pj} a_{qj} x_p x_q =$$
$$= (k-\lambda)(x_1^2 + \ldots + x_v^2) + \lambda(x_1 + \ldots + x_v)^2.$$

Zachodzi również następująca, łatwa do bezpośredniego sprawdzenia tożsamość

$$(b_1^2 + b_2^2 + b_3^2 + b_4^2)(x_1^2 + x_2^2 + x_3^2 + x_4^2) = y_1^2 + y_2^2 + y_3^2 + y_4^2, \tag{4.3}$$

gdzie

$$\begin{aligned} y_1 &= b_1 x_1 - b_2 x_2 - b_3 x_3 - b_4 x_4, \\ y_2 &= b_2 x_1 + b_1 x_2 - b_4 x_3 + b_3 x_4, \\ y_3 &= b_3 x_1 + b_4 x_2 + b_1 x_3 - b_2 x_4, \\ y_4 &= b_4 x_1 - b_3 x_2 + b_2 x_3 + b_1 x_4. \end{aligned} \tag{4.4}$$

Ta niezbyt przejrzysta na pierwszy rzut oka tożsamość ma ciekawą interpretację, w której występujące w niej sumy kwadratów traktowane są jako moduły pewnych kwaternionów (p. zad. 19). Będziemy korzystali również z klasycznego twierdzenia Lagrange'a, które mówi, iż każdą liczbę naturalną n można przedstawić w postaci $b_1^2 + b_2^2 + b_3^2 + b_4^2$ dla pewnych liczb całkowitych b_1, b_2, b_3, b_4. Dowód tego twierdzenia można znaleźć na przykład w książce Sierpińskiego [1, str. 163] (zauważmy, że na mocy tożsamości (4.3), twierdzenia tego wystarczyłoby dowieść dla liczb n pierwszych).

Tożsamość (4.2) możemy przepisać w postaci

$$L_1^2 + \ldots + L_v^2 = n(x_1^2 + \ldots + x_v^2) + \lambda(x_1 + \ldots + x_v)^2. \tag{4.5}$$

O liczbie v założyliśmy, że jest nieparzysta, możliwe są więc dwa przypadki: $v \equiv 1 \pmod 4$ lub $v \equiv 3 \pmod 4$.

Przypadek 1: $v \equiv 1 \pmod 4$. Składniki sumy $x_1^2 + \ldots + x_v^2$ występującej w tożsamości (4.5) grupujemy po cztery. Ponieważ $v \equiv 1 \pmod 4$, ostatni składnik pozostaje niewykorzystany. Przedstawiając, zgodnie z twierdzeniem Lagrange'a, liczbę n w postaci $b_1^2 + b_2^2 + b_3^2 + b_4^2$ i używając tożsamości (4.3) $(v-1)/4$ razy otrzymujemy

$$n(x_i^2 + x_{i+1}^2 + x_{i+2}^2 + x_{i+3}^2) = y_i^2 + y_{i+1}^2 + y_{i+2}^2 + y_{i+3}^2$$

dla $i = 1, 5, \ldots, v-4$. Zdefiniujemy dodatkowo $y_v = x_v$. Tożsamość (4.5) przyjmuje wtedy formę

$$L_1^2 + \ldots + L_v^2 = y_1^2 + \ldots + y_{v-1}^2 + n y_v^2 + \lambda w^2, \tag{4.6}$$

gdzie $w = x_1 + \ldots + x_v$. Łatwo sprawdzić, że wyznacznik macierzy

(4.7)
$$B = \begin{bmatrix} b_1 & -b_2 & -b_3 & -b_4 \\ b_2 & b_1 & -b_4 & b_3 \\ b_3 & b_4 & b_1 & -b_2 \\ b_4 & -b_3 & b_2 & b_1 \end{bmatrix}$$

układu równań (4.4) jest równy $(b_1^2+b_2^2+b_3^2+b_4^2)^2 = n^2$ – wystarczy w tym celu zauważyć, że $BB^T = (b_1^2+b_2^2+b_3^2+b_4^2)I = nI$. Wynika stąd, że możemy jednoznacznie przedstawić $x_1, \ldots, x_v$, a w konsekwencji również $L_1, \ldots, L_v$, w, jako wymierne formy liniowe (tzn. formy liniowe o współczynnikach wymiernych) zmiennych $y_1, \ldots, y_v$. Zakładamy w dalszym ciągu, że w zależności (4.6) zmienne $x_1, \ldots, x_v$ występujące w $L_1, \ldots, L_v, w$ wyrażone zostały przez odpowiednie wymierne formy liniowe zmiennych $y_1, \ldots, y_v$. Niech, w szczególności, $L_1 = c_{11}y_1 + \ldots + c_{1v}y_v$. Przyjmijmy $y_1 = L_1$, jeśli $c_{11} \neq 1$, i $y_1 = -L_1$ w przypadku przeciwnym. Mamy wówczas $L_1^2 = y_1^2$ i z (4.6) otrzymujemy tożsamość

(4.8)
$$L_2^2 + \ldots + L_v^2 = y_2^2 + \ldots + y_{v-1}^2 + ny_v^2 + \lambda w^2,$$

prawdziwą dla dowolnych $y_2, \ldots, y_v$. Po każdej stronie równości występuje tu suma kwadratów pewnych wymiernych form liniowych zmiennych $y_2, \ldots, y_v$, zmienna y_1 została bowiem wyrażona jako

$$y_1 = \frac{c_{12}}{1-c_{11}} y_2 + \ldots + \frac{c_{1v}}{1-c_{11}} y_v \quad (\text{przypadek } c_{11} \neq 1)$$

lub

$$y_1 = -\frac{c_{12}}{2} y_2 - \ldots - \frac{c_{1v}}{2} y_v \quad (\text{przypadek } c_{11} = 1).$$

Kontynuując w analogiczny sposób opisany powyżej proces nakładania pewnych zależności, wyrażonych przez odpowiednie wymierne formy liniowe, na zmienne niezależne $y_1, \ldots y_v$ w tożsamości (4.6) eliminujemy kolejno $y_2, \ldots, y_{v-1}$ i dochodzimy do tożsamości

$$L_v^2 = ny_v^2 + \lambda w^2,$$

w której L_v ma postać $\frac{p}{q} y_v$, zaś w postać $\frac{s}{t} y_v$ dla pewnych liczb całkowitych p, q, s, t. Przyjmując $y_v = qt$ widzimy, że równanie

(4.9)
$$z^2 = nx^2 + \lambda y^2$$

ma rozwiązanie całkowite $x = qt \neq 0$, $y = sq$, $z = pt$. Założyliśmy, że $v \equiv 1 \pmod 4$, a więc $(v-1)/2$ jest liczbą parzystą i równanie (4.9) możemy przedstawić w równoważnej formie

$$z^2 = nx^2 + (-1)^{(v-1)/2} \lambda y^2.$$

Przypadek 2: $v \equiv 3 \pmod 4$. Wprowadzamy nową zmienną x_{v+1} i dodajemy nx_{v+1}^2 do obu stron równości (4.5). Grupując składniki x_i^2 po cztery i korzystając z tożsamości (4.3) dochodzimy w podobny sposób jak poprzednio do tożsamości

$$L_1^2 + \ldots + L_v^2 + nx_{v+1}^2 = y_1^2 + \ldots + y_{v+1}^2 + \lambda w^2.$$

Również w analogiczny sposób jak w poprzednim przypadku otrzymujemy stąd tożsamość

$$nx^2 = y_{v+1}^2 + \lambda w^2,$$

gdzie zarówno x jak i w ma postać iloczynu zmiennej y_{v+1} przez pewną liczbę wymierną. Przyjmując y_{v+1} równe iloczynowi mianowników tych liczb wymiernych, wnioskujemy stąd, że równanie

$$z^2 = nx^2 - \lambda y^2 \tag{4.10}$$

ma rozwiązanie w liczbach całkowitych x, y, z, gdzie $z \neq 0$. Liczba $(v-1)/2$ jest teraz nieparzysta, równanie (4.10) możemy więc przedstawić w równoważnej postaci

$$z^2 = nx^2 + (-1)^{(v-1)/2} \lambda y^2. \quad \square$$

Nie wiadomo czy warunki konieczne z twierdzenia Brucka–Rysera–Chowli, wraz z równością $\lambda(v-1) = k(k-1)$, są wystarczające dla istnienia konfiguracji kwadratowej o parametrach v, k, λ. Warto zauważyć, że gdyby tak było, to istniałaby płaszczyzna rzutowa rzędu 10, tzn. konfiguracja o parametrach $v = 111$, $k = 11$, $\lambda = 1$. Istotnie, równanie (4.1) przyjmuje w tym przypadku postać $z^2 = 10x^2 - y^2$ i ma rozwiązanie $x = y = 1$, $z = 3$.

W dowodzie twierdzenia Brucka–Rysera–Chowli korzystaliśmy jedynie z tego, że elementy macierzy A są wymierne. Warunki podane w twierdzeniu są więc konieczne dla istnienia macierzy A o elementach wymiernych spełniającej równanie

$$AA^T = (k-\lambda)I + \lambda J.$$

Można również wykazać, że w przypadku macierzy o elementach wymiernych warunki te są wystarczające dla istnienia rozwiązania powyższego równania (zakładamy oczywiście $\lambda(v-1) = k(k-1)$). Dowód jest jednak trudny i korzysta z pewnych głębokich faktów dotyczących form kwadratowych (por. M. Hall [3]).

Zastosujemy teraz twierdzenie Brucka–Rysera–Chowli do dowodu nieistnienia pewnych konfiguracji kwadratowych.

TWIERDZENIE 4.2. *Nie istnieje płaszczyzna rzutowa rzędu 6.*

Dowód. Płaszczyzna taka byłaby konfiguracją kwadratową o parametrach $v = n^2+n+1 = 43$, $k = n+1 = 7$, $\lambda = 1$. Wobec twierdzenia Brucka–Rysera–Chowli wystarczy wykazać, że równanie $z^2 = 6x^2 + (-1)^{(43-1)/2} y^2$, czyli

$$6x^2 = y^2 + z^2, \tag{4.11}$$

nie ma nietrywialnych rozwiązań. Udowodnimy to niewprost. Załóżmy zatem, że dla pewnych liczb całkowitych x, y, z nie wszystkich równych zeru nasze równanie jest spełnione. Bez zmniejszenia ogólności możemy zakładać, że liczby x, y, z nie mają żadnego wspólnego dzielnika większego od jedności. Mamy $3|6x^2$, a więc y^2+z^2 musi być podzielne przez 3. Lecz stąd wynika, że zarówno y jak i z są podzielne przez 3. Istotnie, jeśli $y \equiv a \pmod 3$ oraz $z \equiv b \pmod 3$, przy czym $0 \leqslant a, b \leqslant 2$, to $y^2+z^2 \equiv a^2+b^2 \equiv 0 \pmod 3$, co jest możliwe jedynie, jeśli $a = b = 0$. Skoro y i z są podzielne przez 3, to liczby y^2 i z^2, a w konsekwencji również y^2+z^2 i $6x^2$, są podzielne przez 9. Zatem $3|2x^2$ i 3 jest wspólnym dzielnikiem liczb x, y, z. Otrzymana sprzeczność dowodzi, że równanie (4.11) nie ma niezerowych rozwiązań całkowitych. □

Zauważmy, że $6 = 0^2+1^2+1^2+2^2$. Nieistnienie płaszczyzny rzutowej rzędu 6 udowodniliśmy więc bez powoływania się na twierdzenie Lagrange'a.

Zajmiemy się teraz bliżej równaniem (4.1). W tym celu przypomnimy najpierw pewne definicje i fakty z elementarnej teorii liczb. Niech a, m będą względnie pierwszymi niezerowymi liczbami całkowitymi. Będziemy mówili, że a jest *resztą kwadratową modulo m*, jeśli kongruencja $x^2 \equiv a \pmod m$ ma rozwiązanie, oraz *nieresztą kwadratową modulo m* w przeciwnym przypadku. Niech a, b, c będą niezerowymi liczbami całkowitymi, z których nie wszystkie są tego samego znaku. Załóżmy, że liczby te są wolne od kwadratów (tzn. żadna z nich nie jest podzielna przez kwadrat liczby pierwszej), oraz że $(a, b) = (b, c) = (a, c) = 1$. Równanie diofantyczne

$$ax^2+by^2+cz^2 = 0 \tag{4.12}$$

zwane jest wtedy *równaniem Legendre'a*. Znany jest następujący warunek istnienia nietrywialnego (tzn. różnego od $x = y = z = 0$) rozwiązania tego równania:

TWIERDZENIE 4.4 (Legendre). *Równanie* (4.12) *ma nietrywialne rozwiązanie wtedy i tylko wtedy, gdy liczby* $-bc$, $-ac$, $-ab$ *są resztami kwadratowymi modulo odpowiednio* a, b, c.

Pełny dowód można znaleźć w podręczniku teorii liczb (p. np. Nagell [1]). My jednakże będziemy korzystali jedynie z faktu, iż warunki podane w twierdzeniu są konieczne dla istnienia nietrywialnego rozwiązania równania (4.12). Aby pokazać tę część twierdzenia, zauważmy, że z (4.12) wynika

$$-bcz^2 \equiv (by)^2 \pmod a. \tag{4.13}$$

Możemy zakładać, że liczby x, y, z, będące nietrywialnym rozwiązaniem równania (4.12), nie mają wspólnego dzielnika pierwszego. Wykażemy teraz, że $(a, z) = 1$. Przypuśćmy w tym celu, że $p|a$ oraz $p|z$ dla pewnej liczby pierwszej p. Wówczas $p|by^2$, a więc $p|y$, gdyż $p|a$ i $(a, b) = 1$. Wynika stąd, że $p^2|by^2$, $p^2|cz^2$, a więc również $p^2|ax^2$ i w konsekwencji $p|x$, jako że a jest wolne od kwadratów. Otrzymana sprzeczność z założeniem, iż x, y, z nie mają wspólnego dzielnika pierwszego dowodzi, że $(a, z) = 1$. Skoro tak, to istnieje liczba z^* taka, że $z^*z \equiv$

$\equiv 1 \pmod a$. Równanie (4.13) możemy więc przekształcić do postaci

$$-bc \equiv (byz^*)^2 \pmod a,$$

co dowodzi, że $-bc$ jest resztą kwadratową modulo a. Podobne kongruencje dla $-ac$, $-ab$ wynikają z symetrii równania (4.12). □

Wykażemy teraz, że równanie

$$z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2 \tag{4.14}$$

jest równoważne pewnemu równaniu Legendre'a; przez równoważność rozumiemy tu fakt, iż albo oba równania mają rozwiązania nietrywialne, albo żadne z nich.

Oznaczmy przez n' część wolną od kwadratów liczby n, tzn. $n' = n/k$, gdzie k jest największym kwadratem dzielącym n. Niech λ' będzie częścią wolną od kwadratów liczby λ, zaś $s = (n', \lambda')$. Równanie (4.14) jest równoważne równaniu

$$s^2 z^2 = n'x^2 + (-1)^{(v-1)/2}\lambda' y^2,$$

(p. zad. 23), czyli równaniu Legendre'a

$$\frac{n'}{s}x^2 + (-1)^{(v-1)/2}\frac{\lambda'}{s}y^2 - sz^2 = 0. \tag{4.15}$$

Otrzymujemy stąd następującą „efektywną" wersję twierdzenia Brucka–Rysera–Chowli:

TWIERDZENIE 4.5. *Jeśli istnieje konfiguracja kwadratowa o parametrach v, k, λ, gdzie v jest nieparzyste, to liczby*

$$(-1)^{(v-1)/2}\lambda', \quad n', \quad (-1)^{(v+1)/2}\frac{\lambda' n'}{s^2}$$

są resztami kwadratowymi modulo odpowiednio

$$\frac{n'}{s}, \quad \frac{\lambda'}{s}, \quad s,$$

gdzie n', λ' są częściami wolnymi od kwadratów liczb $n = k-\lambda$, λ, zaś $s = (n', \lambda')$. □

Na zakończenie tego paragrafu zastosujemy twierdzenie 4.5 do dowodu nieistnienia płaszczyzn rzutowych dla nieskończenie wielu wartości parametru n.

TWIERDZENIE 4.6. *Jeśli $n \equiv 1$ lub $2 \pmod 4$ oraz część wolna od kwadratów liczby n dzieli się przez pewną liczbę pierwszą $p \equiv 3 \pmod 4$, to nie istnieje płaszczyzna rzutowa rzędu n.*

Dowód. Parametr v płaszczyzny rzutowej jest zawsze nieparzysty, gdyż $v = n^2+n+1$. Mamy $\lambda = \lambda' = s = 1$, a więc wystarczy rozpatrywać tylko pierwszy z warunków twierdzenia 4.5. Założenie $n \equiv 1$ lub $2 \pmod 4$ oznacza, że $(v-1)/2$ jest nieparzyste, zatem jeśli płaszczyzna rzutowa istnieje, to -1 jest resztą kwadratową

modulo n', a więc również modulo p. Lecz z elementarnej teorii liczb wiadomo, że -1 jest nieresztą kwadratową modulo p, jeśli $p \equiv 3 \pmod 4$ (por. Dodatek, tw. 34). □

Twierdzenie to wyklucza w szczególności istnienie płaszczyzn rzutowych rzędu $2p$, p pierwsze, $p \equiv 3 \pmod 4$. Nie istnieją zatem płaszczyzny rzędu $n = 6, 14, 22, 38, 46$, oraz dla nieskończenie wielu innych wartości n, jako że istnieje nieskończenie wiele liczb pierwszych postaci $4k+3$ (por. Sierpiński [1], str. 98).

Z teorii liczb wiadomo, że jeśli część wolna od kwadratów liczby n nie dzieli się przez żadną liczbę pierwszą postaci $4k+3$, to n jest sumą dwóch kwadratów liczb całkowitych (p. Sierpiński [1], str. 160). Zatem dla $n \equiv 1$ lub $2 \pmod 4$ warunkiem koniecznym istnienia płaszczyzny rzutowej rzędu n jest istnienie liczb całkowitych a, b takich, że $a^2+b^2 = n$.

§ 5. Zbiory różnicowe

Jedna z podstawowych metod konstrukcji konfiguracji kwadratowych polega na wykorzystaniu pojęcia tzw. zbioru różnicowego.

Niech G będzie dowolną, niekoniecznie przemienną grupą o v elementach. Działanie grupowe będziemy oznaczali symbolem $\cdot$, zaś jedynkę grupy przez 1.

Zbiorem różnicowym o parametrach v, k, λ w grupie G będziemy nazywali dowolny podzbiór k-elementowy $D = \{a_1, \ldots, a_k\} \subseteq G$ o tej własności, że dla każdego elementu $d \in G$ różnego od jedynki istnieje dokładnie λ par $\langle a_i, a_j \rangle \in D \times D$ takich, że

(5.1) $$a_i a_j^{-1} = d.$$

Jeśli G jest grupą cykliczną — ogólniej, dowolną grupą przemienną — to zgodnie z tradycją działanie grupowe oznaczamy przez $+$. W takim przypadku $D \subseteq G$ jest zbiorem różnicowym, jeśli każdy element niezerowy $d \in G$ można otrzymać dokładnie λ sposobami jako różnicę $d = a_i - a_j$, gdzie a_i, $a_j \in D$. Stąd nazwa „zbiór różnicowy".

Zbiory różnicowe w grupach cyklicznych nazywane są *cyklicznymi zbiorami różnicowymi*. Oczywiście badając cykliczne zbiory różnicowe możemy zakładać, że G jest grupą $\boldsymbol{Z}_v$ reszt modulo v.

Przykładem cyklicznego zbioru różnicowego jest zbiór $D = \{0, 1, 3\}$ w grupie $\boldsymbol{Z}_7$ — oznaczamy go krótko przez $\{0, 1, 3\} \bmod 7$. Łatwo to sprawdzić w poniższej tablicy zawierającej wszystkie możliwe różnice $a-b$ dla a, $b \in D$.

a \ b	0	1	3
0	0	6	4
1	1	0	5
3	3	2	0

Innymi przykładami cyklicznych zbiorów różnicowych są

$\{0, 3, 5, 6\} \bmod 7$ $(v = 7,\ k = 4, \lambda = 2)$,
$\{0, 2, 3, 4, 8\} \bmod 11$ $(v = 11, k = 5, \lambda = 2)$,
$\{0, 1, 3, 9\} \bmod 13$ $(v = 13, k = 4, \lambda = 1)$,
$\{0, 3, 4, 5, 6, 8, 10, 15, 16\} \bmod 19$ $(v = 19, k = 9, \lambda = 4)$.

Podamy teraz przykład zbioru różnicowego w grupie (niecyklicznej) $G = \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2$. Zbiór ten ma postać

$$D = \{0000, 0001, 0010, 0100, 1000, 1111\}$$

(przy wypisywaniu elementów grupy G pomijamy nawiasy i przecinki, pisząc 0000 zamiast $\langle 0, 0, 0, 0\rangle$ itd.). Analizując poniższą tabelkę różnic $a-b$ możemy łatwo się przekonać, że D jest rzeczywiście zbiorem różnicowym o parametrach $v = 16$, $k = 6$, $\lambda = 2$:

a \ b	0000	0001	0010	0100	1000	1111
0000	0000	0001	0010	0100	1000	1111
0001	0001	0000	0011	0101	1001	1110
0010	0010	0011	0000	0110	1010	1101
0100	0100	0101	0110	0000	1100	1011
1000	1000	1001	1010	1100	0000	0111
1111	1111	1110	1101	1011	0111	0000

Zamiast konstruować tablicę różnic możemy również rozumować w następujący sposób: Suma wszystkich sześciu elementów zbioru D jest równa 0000. Łatwo też widzieć, że suma żadnych dwóch, a więc i żadnych czterech elementów, nie jest równa 0000. Jeśli więc dla dwu różnych par $\langle a_i, a_j\rangle, \langle a_k, a_l\rangle \in D \times D$ mamy $a_i + a_j = a_k + a_l \neq 0$, to musi być $i = l$, $j = k$ (zauważmy, że w naszej grupie $-a = a$). Zatem wśród 30 niezerowych różnic $a_i - a_j$ $(a_i, a_j \in D, i \neq j)$ każdy element niezerowy występuje dokładnie dwa razy.

W dowolnej grupie G mamy następujące zbiory różnicowe, które będziemy nazywali *zdegenerowanymi*:

(a) $D = \emptyset$ $(k = 0, \lambda = 0)$,
(b) $D = \{a\}, a \in G$ $(k = 1, \lambda = 0)$,
(c) $D = G$ $(k = v, \lambda = v)$,
(d) $D = G \setminus \{a\}, a \in G$ $(k = v-1, \lambda = v-2)$.

Zauważmy, że każdą różnicę d można otrzymać na v sposobów jako $(dx)x^{-1}$ $(x \in G)$. Stąd $\lambda = v$ w przypadku (c). Jeśli z grupy G usuniemy element a, to odpadają dwa sposoby: $(da)a^{-1}$ oraz $a(d^{-1}a)^{-1}$. Stąd $\lambda = v-2$ w przypadku (d).

Dla dowolnego podzbioru D grupy G oraz dowolnego elementu $x \in G$ będziemy używali oznaczeń

$$Dx = \{ax\colon a \in D\}, \qquad xD = \{xa\colon a \in D\}.$$

Jeśli G jest grupą przemienną, to oczywiście $Dx = xD$. Sens oznaczeń $D+x$, $x+D$ jest oczywisty. Zbiór Dx, jak również zbiór xD, będziemy nazywali *przesunięciem podzbioru D*. Z równości

$$(a_i x)(a_j x)^{-1} = a_i x x^{-1} a_j^{-1} = a_i a_j^{-1},$$
$$(x a_i)(x a_j)^{-1} = x a_i a_j^{-1} x^{-1} = x(a_i a_j^{-1})x^{-1}$$

wynika natychmiast, że dowolne przesunięcie zbioru różnicowego jest zbiorem różnicowym o tych samych parametrach (zauważmy, że odwzorowanie $d \mapsto xdx^{-1}$ jest permutacją niezerowych elementów grupy G — jest nawet jej automorfizmem).

Tablica różnic dowolnego zbioru różnicowego o parametrach v, k, λ zawiera k^2 różnic, z których k na przekątnej głównej jest równych zeru. Każdy spośród $v-1$ elementów niezerowych grupy G występuje w tablicy dokładnie λ razy. Otrzymujemy stąd równość

$$\lambda(v-1) = k(k-1). \tag{5.2}$$

Podobieństwo tego wzoru do zależności (2.1) wiążącej ze sobą parametry v, k, λ konfiguracji kwadratowej nie jest przypadkowe. Mamy bowiem następujące twierdzenie:

TWIERDZENIE 5.1. *Niech G będzie dowolną grupą skończoną. Podzbiór $D \subseteq G$ jest zbiorem różnicowym o parametrach v, k, λ wtedy i tylko wtedy, gdy $\langle G, \mathscr{B}\rangle$, gdzie*

$$\mathscr{B} = (Dx\colon\ x \in G), \tag{5.3}$$

jest konfiguracją kwadratową o parametrach v, k, λ (zdegenerowaną wtedy i tylko wtedy, gdy D jest zdegenerowanym zbiorem różnicowym).

Dowód. Ustalmy dowolne dwa różne elementy $g, h \in G$ i oznaczmy $d = gh^{-1}$. Aby udowodnić twierdzenie, wystarczy podać wzajemnie jednoznaczną odpowiedniość między parami $\langle a_i, a_j\rangle \in D \times D$ takimi, że $a_i a_j^{-1} = d$, oraz elementami $x \in G$ takimi, że $g, h \in Dx$. W tym celu przyporządkujmy parze $\langle a_i, a_j\rangle$ element

$$x = a_i^{-1} g. \tag{5.4}$$

Łatwo widać, że różnym parom $\langle a_i, a_j\rangle$ spełniającym $a_i a_j^{-1} = d$ odpowiadają różne elementy x, przy czym

$$g = a_i x \in Dx,$$
$$h = d^{-1} g = (a_i a_j^{-1})^{-1} g = a_j a_i^{-1} g = a_j x \in Dx.$$

Na odwrót, jeśli $g, h \in Dx$, to istnieją elementy $a_i, a_j \in D$ takie, że $g = a_i x$, $h = a_j x$. Mamy wówczas

$$a_i a_j^{-1} = (gx^{-1})(hx^{-1})^{-1} = gx^{-1} x h^{-1} = gh^{-1} = d.$$

Przyporządkowanie określone przez (5.4) jest więc wzajemnie jednoznaczne. □

O konfiguracji $\langle G, \mathscr{B}\rangle$ określonej wzorem (5.3) będziemy mówili, że jest *wyznaczona przez zbiór różnicowy D*.

Dla przykładu, konfiguracja wyznaczona przez zbiór różnicowy $\{0, 2, 3, 4, 8\}$ mod 11 w grupie Z_{11} jest następująca:

$$
\begin{array}{c}
 \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \\ 10
\end{array}
\begin{array}{c}
\begin{array}{ccccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{array} \\
\begin{bmatrix}
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\
0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\
1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\
1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1
\end{bmatrix}
\end{array}.
$$

W powyższej macierzy każda następna kolumna powstaje z poprzedniej przez cykliczne przesunięcie w dół o jedną pozycję. Element a_{ij} jest równy jedynce, jeśli $i-j \in D$, oraz zeru w przeciwnym przypadku.

Konfiguracje wyznaczone przez cykliczne zbiory różnicowe będziemy nazywali *konfiguracjami cyklicznymi*.

Regularność struktury konfiguracji określonej przez (5.3) znajduje swoje odbicie w grupie wszystkich automorfizmów tej konfiguracji. Aby to dokładnie opisać, będziemy potrzebowali paru pomocniczych definicji.

Będziemy mówili, że podgrupa G grupy wszystkich permutacji zbioru n-elementowego X jest *regularna*, jeśli dla dowolnych elementów $x, y \in X$ istnieje dokładnie jedna permutacja $g \in G$ taka, że $g(x) = y$. Równoważnie możemy powiedzieć, że grupa G jest *regularna*, jeśli jest rzędu n (tzn. $|G| = n$) oraz jest *przechodnia* (tzn. dla dowolnych $x, y \in X$ istnieje g takie, że $g(x) = y$). Przykładem regularnej grupy permutacji zbioru $X = \{0, \ldots, n-1\}$ jest grupa cykliczna generowana przez permutację $x \mapsto x+1 \pmod n$. Jeśli dla regularnej grupy permutacji G ustalimy pewien element bazowy $x_0 \in X$, to każdą permutację $g \in G$ możemy identyfikować z elementem $g(x_0)$. Sam punkt x_0 odpowiada oczywiście jedynce grupy G. Jeśli w powyższym przykładzie cyklicznej grupy permutacji wybierzemy 0 jako element bazowy, to permutacji $x \mapsto x+k \pmod n$ odpowiada element $k \pmod n$.

Będziemy mówili, że pewna grupa automorfizmów* konfiguracji kwadratowej $\langle X, \mathscr{B}\rangle$ jest *regularna*, jeśli działa ona na punktach tej konfiguracji jako regularna

---

* Przez grupę automorfizmów będziemy rozumieli zawsze podgrupę grupy wszystkich automorfizmów.

grupa permutacji. W przypadku konfiguracji kwadratowych bloki są parami różne, a więc możemy utożsamiać automorfizm z jego działaniem na punktach. Mówimy, że automorfizm α *ustala* punkt x (blok B), jeśli $(x)\alpha = x$ ($(B)\alpha = B$).

LEMAT 5.2 (Parker). *Dowolny automorfizm konfiguracji kwadratowej ustala tę samą liczbę punktów co bloków.*

Dowód. Jeśli α jest automorfizmem pewnej konfiguracji kwadratowej o macierzy incydencji A, to jest spełniona równość

$$P^{-1}AQ = A, \tag{5.5}$$

gdzie $P = [p_{ij}]$ i $Q = [q_{ij}]$ są macierzami permutacyjnymi określonymi następująco: $p_{ij} = 1$, jeśli α przeprowadza j-ty punkt na i-ty, oraz $p_{ij} = 0$ w przeciwnym przypadku; podobnie dla macierzy Q. Automorfizm α ustala $\operatorname{tr} P = \sum_i p_{ii}$ punktów i $\operatorname{tr} Q = \sum_i q_{ii}$ bloków. Wiemy, że macierz incydencji konfiguracji kwadratowej jest nieosobliwa, z (5.5) otrzymujemy więc

$$Q = A^{-1}PA,$$

a stąd

$$\operatorname{tr} Q = \operatorname{tr} A^{-1}PA = \operatorname{tr} PAA^{-1} = \operatorname{tr} P,$$

jako że dla dowolnych macierzy kwadratowych

$$B = [b_{ij}], \qquad C = [c_{ij}]$$

mamy

$$\operatorname{tr} BC = \sum_i \sum_j b_{ij}c_{ji} = \sum_j \sum_i c_{ji}b_{ij} = \operatorname{tr} CB. \ \square$$

Zauważmy, że grupa G rzędu $n = |X|$ permutacji zbioru X jest regularna wtedy i tylko wtedy, gdy żaden jej element $g \neq 1$ nie ustala żadnego elementu $x \in X$. Zatem z lematu 5.2 otrzymujemy następujący wniosek.

WNIOSEK 5.3. *Grupa automorfizmów konfiguracji kwadratowej działa jako regularna grupa permutacji zbioru punktów wtedy i tylko wtedy, gdy działa jako regularna grupa permutacji zbioru bloków.*

Istnieje ścisły związek między grupą G a grupą automorfizmów konfiguracji wyznaczonej przez zbiór różnicowy w grupie G. Zachodzi mianowicie następujące

TWIERDZENIE 5.4. *Jeśli D jest zbiorem różnicowym w grupie G, to konfiguracja wyznaczona przez D ma regularną grupę automorfizmów izomorficzną z G.*

Na odwrót, załóżmy, że G jest regularną grupą automorfizmów pewnej konfiguracji $\langle X, \mathscr{B}\rangle$. Ustalmy pewien punkt $x_0 \in X$ oraz pewien blok $B \in \mathscr{B}$ i załóżmy, że

$$B = \{(x_0)g_1, \ldots, (x_0)g_k\},$$

gdzie $g_1, \ldots, g_k$ są elementami grupy G (jednoznacznie wyznaczonymi przez B na

mocy regularności G). Wówczas $\{g_1, \ldots, g_k\}$ *jest zbiorem różnicowym w G, który wyznacza z dokładnością do izomorfizmu konfigurację* $\langle X, \mathscr{B}\rangle$.

Dowód. Niech D będzie zbiorem różnicowym w G i niech $\langle G, \mathscr{B}\rangle$ będzie konfiguracją wyznaczoną przez D. Dowolny element $g \in G$ określa automorfizm α_g tej konfiguracji, który przeprowadza punkt h na punkt hg oraz blok Dx na blok Dxg, dla dowolnych $h, x \in G$. Łatwo zauważyć, że elementowi yz grupy G odpowiada złożenie $\alpha_y \alpha_z$, tzn. $\alpha_{yz} = \alpha_y \alpha_z$. Różnym elementom $g \in G$ odpowiadają oczywiście różne automorfizmy α_g, grupa G wyznacza więc grupę automorfizmów izomorficzną z G. Grupa ta jest regularna, gdyż jedynym automorfizmem przeprowadzającym y na z jest $\alpha_{y^{-1}z}$.

Niech teraz G będzie regularną grupą automorfizmów konfiguracji $\langle X, \mathscr{B}\rangle$. Będziemy identyfikowali dowolny punkt $x \in X$ z automorfizmem $g \in G$ takim, że $x = (x_0)g$ – przyjmujemy zatem, że $X = G$. Niech $B = \{g_1, \ldots, g_k\}$ będzie pewnym blokiem naszej konfiguracji i niech $\mathscr{C} = (Bg\colon g \in G)$. Wykażemy, że $\langle G, \mathscr{C}\rangle$ pokrywa się z konfiguracją $\langle G, \mathscr{B}\rangle$. Wystarczy w tym celu zauważyć, że Bg jest blokiem konfiguracji $\langle G, \mathscr{B}\rangle$, na który automorfizm g przeprowadza blok B. Wobec regularności grupy G zbiór $\mathscr{C}$ pokrywa się ze zbiorem wszystkich bloków konfiguracji $\langle G, \mathscr{B}\rangle$. Na mocy twierdzenia 5.1 zbiór B jest zbiorem różnicowym w G. Zbiór ten wyznacza konfigurację $\langle G, \mathscr{C}\rangle$ izomorficzną z $\langle X, \mathscr{B}\rangle$. □

Dwa pytania nasuwają się w związku z twierdzeniami 5.1 i 5.4. Po pierwsze: czy każda konfiguracja jest wyznaczona przez pewien zbiór różnicowy, tzn. czy każda konfiguracja ma regularną grupę automorfizmów? Po drugie: czy regularna grupa automorfizmów konfiguracji wyznaczonej przez zbiór różnicowy jest grupą jej wszystkich automorfizmów?

Odpowiedzi na oba te pytania są negatywne. Znane są konfiguracje kwadratowe bez regularnej grupy automorfizmów, na przykład konfiguracja kwadratowa o parametrach $v = 31$, $k = 10$, $\lambda = 3$ (nr 40 na liście M. Halla [3]; 31 jest liczbą pierwszą, zatem jedyna grupa rzędu 31 jest cykliczna, natomiast łatwo można sprawdzić, że konfiguracja ta nie jest cykliczna). W dalszym ciągu zobaczymy również, że na ogół dla zbioru różnicowego istnieje tzw. mnożnik, który odpowiada pewnemu dodatkowemu automorfizmowi konfiguracji wyznaczonej przez ten zbiór różnicowy.

Będziemy mówili, że dwa zbiory różnicowe $D \subseteq G$ i $E \subseteq H$ są *równoważne*, jeśli istnieje izomorfizm grup G i H, który przeprowadza D na E. W szczególności każdy automorfizm grupy G przeprowadza D na pewien równoważny zbiór różnicowy w G. Oczywiście, równoważne zbiory różnicowe wyznaczają izomorficzne konfiguracje kwadratowe.

§ 6. Konfiguracje i zbiory różnicowe wyznaczone przez geometrie skończone

W paragrafie 2 pokazaliśmy, że skończoną płaszczyznę rzutową rzędu n można traktować jako konfigurację kwadratową o parametrach $v = n^2+n+1$, $k = n+1$,

$\lambda = 1$. Obecnie podamy parę innych przykładów konstrukcji konfiguracji i zbiorów różnicowych z pewnych geometrii skończonych. Ograniczymy się tu do geometrii rzutowych $PG(n, q)$ oraz afinicznych $AG(n, q)$. Wszystkie niezbędne pojęcia dotyczące tych geometrii można znaleźć w rozdziale 1, § 12. Będziemy też korzystali z pewnych faktów dotyczących ciał skończonych, które omówione są szczegółowo w Dodatku.

Przypomnijmy, że n-wymiarową geometrię rzutową $PG(n, q)$ otrzymujemy rozważając $(n+1)$-wymiarową przestrzeń wektorową $V(n+1, q)$ nad ciałem $GF(q)$, złożoną z wektorów postaci

(6.1) $$x = \langle a_n, a_{n-1}, \ldots, a_0 \rangle, \quad a_i \in GF(q),$$

oraz utożsamiając dwa wektory niezerowe x, y, jeśli $y = cx$ dla pewnego $c \in GF(q)$, $c \neq 0$. Klasy równoważnych wektorów niezerowych tworzą punkty geometrii $PG(n, q)$. Każdy punkt jest reprezentowany przez $q-1$ wektorów postaci (6.1), wszystkich punktów jest więc $(q^{n+1}-1)/(q-1)$. Podprzestrzeń r-wymiarowa geometrii $PG(n, q)$ składa się z $(q^{r+1}-1)/(q-1)$ punktów reprezentowanych przez wektory niezerowe z pewnej $(r+1)$-wymiarowej podprzestrzeni przestrzeni $V(n+1, q)$. Podprzestrzenie $(n-1)$-wymiarowe geometrii $PG(n, q)$ nazywamy *hiperpłaszczyznami*.

Udowodnimy teraz twierdzenie określające pewną rodzinę nieskończoną konfiguracji cyklicznych. Zauważmy, iż na mocy rozważań poprzedniego paragrafu cykliczność konfiguracji jest równoważna istnieniu regularnej cyklicznej grupy automorfizmów.

Niech $q = p^m$, gdzie p jest liczbą pierwszą a $m > 0$.

TWIERDZENIE 6.1 (Singer [1]). *Geometria rzutowa $PG(n, q)$ określa konfigurację kwadratową o parametrach*

(6.2) $$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^n-1}{q-1}, \quad \lambda = \frac{q^{n-1}-1}{q-1},$$

której punktami są punkty, blokami zaś hiperpłaszczyzny tej geometrii. Konfiguracja ta jest cykliczna.

Dowód. Pierwsza część twierdzenia jest łatwa. Geometria $PG(n, q)$ zawiera v punktów i tyle samo hiperpłaszczyzn, każda hiperpłaszczyzna zawiera k punktów, a przecięcie dwóch różnych hiperpłaszczyzn jest podprzestrzenią wymiaru $n-2$, zawiera więc λ punktów, gdzie v, k, λ są określone wzorami (6.2). Na mocy twierdzenia 3.1 hiperpłaszczyzny określają konfigurację kwadratową o parametrach v, k, λ.

Wykażemy teraz, że ta konfiguracja jest cykliczna. Niech a będzie elementem pierwotnym ciała $GF(q^{n+1})$, tzn. elementem, którego potęgi przebiegają wszystkie elementy niezerowe ciała. Każdy element $b \in GF(q^{n+1})$ można przedstawić jednoznacznie w postaci

(6.3) $$b = b_n a^n + b_{n-1} a^{n-1} + \ldots + b_1 a + b_0, \quad b_i \in GF(q)$$

(p. Dodatek). Przedstawienie to pozwala przyporządkować wzajemnie jednoznacznie każdemu elementowi $b \in GF(q^{n+1})$ wektor $F(b) = \langle b_n, \ldots, b_0 \rangle$ przestrzeni $V(n+1, q)$. Łatwo widać, że

(6.4) $$F(cb) = cF(b),$$

(6.5) $$F(b_1 + b_2) = F(b_1) + F(b_2)$$

dla dowolnych $b, b_1, b_2 \in GF(q^{n+1})$, $c \in GF(q)$. Innymi słowy, odwzorowanie F określa izomorfizm między ciałem $GF(q^{n+1})$ traktowanym jako przestrzeń liniowa nad podciałem $GF(q)$, a przestrzenią $V(n+1, q)$.

Niech $v = (q^{n+1}-1)/(q-1)$. Wówczas dla dowolnego j

$$(a^{jv})^q = a^{jvq} = a^{jv} a^{jv(q-1)} = a^{jv} a^{j(q^{n+1}-1)} = a^{jv},$$

jako że dla elementu pierwotnego a mamy $a^{q^{n+1}-1} = 1$. Elementy $0, 1, a^v, a^{2v}, \ldots, a^{(q-1)v}$ stanowią więc q różnych pierwiastków równania $x^q = x$ i w konsekwencji tworzą podciało $GF(q)$ ciała $GF(q^{n+1})$ (p. Dodatek, tw. 30). Zatem dla dowolnego całkowitego t mamy $a^{tv} \in GF(q)$ i wobec (6.4)

$$F(a^{i+tv}) = F(a^{tv} a^i) = a^{tv} F(a^i).$$

Stąd łatwo wynika, że wektory $F(a^i)$, $F(a^j)$ reprezentują ten sam punkt geometrii $PG(n, q)$ wtedy i tylko wtedy, gdy $i \equiv j \pmod v$. Jest zatem jasne, że odwzorowanie

(6.5) $$\alpha\colon\ a^i \mapsto a^{i+1}$$

określone na elementach niezerowych ciała $GF(q^{n+1})$ indukuje przesunięcie punktów geometrii $PG(n, q)$ wzdłuż cyklu o długości v, które przeprowadza punkt reprezentowany przez $F(a^i)$ na punkt reprezentowany przez $F(a^{i+1})$. Wykażemy teraz, że odwzorowanie to przeprowadza w $PG(n, q)$ hiperpłaszczyzny na hiperpłaszczyzny. Wystarczy w tym celu udowodnić, że odwzorowanie β określone przez

$$\beta\colon\ F(a^i) \mapsto F(a^{i+1}), \qquad \beta\colon\ \langle 0, \ldots, 0 \rangle \mapsto \langle 0, \ldots, 0 \rangle$$

jest przekształceniem liniowym nieosobliwym przestrzeni $V(n+1, q)$ na siebie. Niech zatem $w_1 = F(a^i)$, $w_2 = F(a^j)$, $c_1, c_2 \in GF(q)$. Z (6.4) i (6.5) wynika, że

$$\begin{aligned} \beta(c_1 w_1 + c_2 w_2) &= \beta\big(c_1 F(a^i) + c_2 F(a^j)\big) = \\ &= \beta\big(F(c_1 a^i + c_2 a^j)\big) = F\big((c_1 a^i + c_2 a^j)a\big) = \\ &= F(c_1 a^{i+1} + c_2 a^{j+1}) = c_1 \beta(w_1) + c_2 \beta(w_2). \end{aligned}$$

Z definicji żaden wektor niezerowy nie przechodzi na zerowy, zatem β jest przekształceniem nieosobliwym.

Udowodniliśmy więc, że odwzorowanie α określone przez (6.6) indukuje automorfizm naszej konfiguracji. Automorfizm ten generuje grupę cykliczną automorfizmów, która jest regularna, gdyż działa jako regularna grupa permutacji na zbiorze punktów. □

Dowód jest zakończony, lecz warto jeszcze uczynić kilka uwag. Z wniosku 5.3 łatwo wynika, że automorfizm indukowany przez α przesuwa również bloki konfiguracji wzdłuż cyklu długości v. Przyjmując punkt reprezentowany przez $F(1)$ jako punkt bazowy oraz przyporządkowując automorfizmowi indukowanemu przez α^k: $a^i \mapsto a^{i+k}$ resztę $k(\text{mod}\, v)$ ustalamy izomorfizm między rozpatrywaną grupą automorfizmów a grupą addytywną reszt modulo v. Załóżmy, że pewien blok naszej konfiguracji składa się z punktów reprezentowanych przez $F(a^{i_1}), \ldots, F(a^{i_k})$. Na mocy twierdzenia 5.4

$$\{i_1, \ldots, i_k\} \bmod v$$

jest zbiorem różnicowym o parametrach określonych wzorami (6.2). Zbiory otrzymane w ten sposób nazywamy *zbiorami różnicowymi Singera*.

Dla obliczenia rozwinięć postaci (6.3) dla elementów $a, a^2, \ldots, a^v$ wygodnie jest skorzystać z pewnego wielomianu

$$P(y) = y^{n+1} + c_n y^n + \ldots + c_1 y + c_0, \qquad c_i \in GF(q)$$

nierozkładalnego nad $GF(q)$ i takiego, że $P(a) = 0$. Wielomian taki zawsze istnieje (jest nawet jednoznacznie wyznaczony przez a, patrz Dodatek). Dzięki równości $P(a) = 0$ możemy dowolny wielomian względem a — na przykład otrzymany przez pomnożenie dwóch wielomianów postaci (6.3) — zredukować modulo $P(a)$.

W szczególności, jeśli

$$a^i = b_n a^n + b_{n-1} a^{n-1} + \ldots + b_1 a + b_0,$$

to

$$a^{i+1} = (b_{n-1} - b_n c_n) a^n + (b_{n-2} - b_n c_{n-1}) a^{n-1} + \ldots + (b_0 - b_n c_1) a - b_n c_0.$$

Rozważmy dla przykładu przypadek $q = 3$, $n = 2$. Ciało $GF(3^3)$ możemy otrzymać jako ciało reszt modulo $P(x) = x^3 + 2x + 1$. Można łatwo sprawdzić, że wielomian ten jest nierozkładalny nad $GF(3)$, oraz że element ciała wyznaczony przez resztę x jest elementem pierwotnym ciała $GF(3^3)$. Oczywiście element ten jest pierwiastkiem wielomianu P. Mamy $v = (3^3 - 1)/(3 - 1) = 13$. Wyznaczmy wektory przestrzeni $V(3, 3)$ odpowiadające elementom $x, x^2, \ldots, x^v$

x^i	$F(x^i)$
x	$\langle 0, 1, 0 \rangle$
x^2	$\langle 1, 0, 0 \rangle$
x^3	$\langle 0, 1, 2 \rangle$
x^4	$\langle 1, 2, 0 \rangle$
x^5	$\langle 2, 1, 2 \rangle$
x^6	$\langle 1, 1, 1 \rangle$
x^7	$\langle 1, 2, 2 \rangle$
x^8	$\langle 2, 0, 2 \rangle$
x^9	$\langle 0, 1, 1 \rangle$
x^{10}	$\langle 1, 1, 0 \rangle$
x^{11}	$\langle 1, 1, 2 \rangle$
x^{12}	$\langle 1, 0, 2 \rangle$
x^{13}	$\langle 0, 0, 2 \rangle$

Potrzebujemy teraz pewnej hiperpłaszczyzny, tzn. podprzestrzeni dwuwymiarowej w $V(3, 3)$. Najłatwiej otrzymać ją jako podprzestrzeń zerową (jądro) pewnego funkcjonału liniowego $f\colon V(3, 3) \to GF(3)$, na przykład określonego następująco:

$$f(b_2, b_1, b_0) = b_0.$$

Funkcjonał ten określa hiperpłaszczyznę w $PG(2, 3)$ złożoną z punktów odpowiadających elementom x, x^2, x^4, x^{10}. Otrzymujemy zatem zbiór różnicowy

$$\{1, 2, 4, 10\} \bmod 13.$$

Przyjmując inne funkcjonały liniowe, np. $f(b_2, b_1, b_0) = b_1$, lub $f(b_2, b_1, b_0) = b_2$ otrzymalibyśmy zbiory różnicowe $\{0, 2, 8, 12\} \bmod 13$ i $\{0, 1, 3, 9\} \bmod 13$. Są one przesunięciami poprzedniego zbioru. Nic w tym dziwnego – z poprzednich rozważań wynika, że dowolne dwie hiperpłaszczyzny można na siebie nałożyć przez cykliczne przesunięcie wzdłuż cyklu wyznaczonego przez $x, x^2, \ldots, x^{13} = x^0$.

Otrzymany przez nas zbiór różnicowy ma parametry $v = 13$, $k = 4$, $\lambda = 1$, a więc odpowiadająca mu konfiguracja to nic innego, jak płaszczyzna rzutowa rzędu 3. Jest to po prostu płaszczyzna rzutowa $PG(2, 3)$ – hiperpłaszczyzny są jej liniami. Ogólnie, konstrukcja opisana w dowodzie twierdzenia Singera dostarcza w przypadku $n = 2$ cyklicznej płaszczyzny rzutowej, tzn. takiej, która odpowiada konfiguracji cyklicznej. Parametry v, k, λ są równe

$$v = (q^3-1)/(q-1) = q^2+q+1,$$
$$k = (q^2-1)/(q-1) = q+1,$$
$$\lambda = (q-1)/(q-1) = 1,$$

zatem otrzymana płaszczyzna rzutowa jest rzędu q. Ponieważ ciało $GF(q)$ istnieje dla dowolnego $q = p^m$, gdzie p jest liczbą pierwszą, a $m > 0$, otrzymujemy następujący wniosek.

Wniosek 6.2. *Dla każdego q będącego potęgą liczby pierwszej istnieje cykliczna płaszczyzna rzutowa rzędu q.* □

Oto zbiory różnicowe odpowiadające tym płaszczyznom dla kilku początkowych wartości q:

q	Zbiór różnicowy
2	$\{0, 1, 3\} \bmod 7$
3	$\{0, 1, 3, 9\} \bmod 13$
$4 = 2^2$	$\{0, 1, 4, 14, 16\} \bmod 21$
5	$\{0, 1, 3, 8, 12, 18\} \bmod 31$
7	$\{0, 1, 3, 13, 32, 36, 43, 52\} \bmod 57$
$8 = 2^3$	$\{0, 1, 3, 7, 15, 31, 36, 54, 63\} \bmod 73$
$9 = 3^2$	$\{0, 1, 3, 9, 27, 49, 56, 61, 77, 81\} \bmod 91$
11	$\{0, 1, 3, 12, 20, 34, 38, 81, 88, 94, 104, 109\} \bmod 133$

Warto wspomnieć, że znane są również niecykliczne płaszczyzny rzutowe (p. M. Hall [3]).

Z geometrii rzutowej $PG(n, q)$ można również otrzymać pewne konfiguracje niekwadratowe. Wystarczy w tym celu przyjąć jako bloki wszystkie podprzestrzenie s-wymiarowe geometrii $PG(n, q)$, $1 \leqslant s \leqslant n-2$. Każda taka podprzestrzeń zawiera $(q^{s+1}-1)/(q-1)$ punktów. Podprzestrzeń s-wymiarową można określić przez odpowiadającą jej podprzestrzeń $(s+1)$-wymiarową przestrzeni $V(n+1, q)$. Podprzestrzeni s-wymiarowych jest więc w $PG(n, q)$ dokładnie $\binom{n+1}{s+1}_q$. Każde dwa punkty geometrii $PG(n, q)$, tzn. każde dwa liniowo niezależne wektory x, y przestrzeni $V(n+1, q)$ wyznaczają podprzestrzeń 1-wymiarową (linię) w $PG(n, q)$. Aby taką linię rozszerzyć do podprzestrzeni s-wymiarowej, należy w $V(n+1, q)$ uzupełnić x, y do bazy przestrzeni $(s+1)$-wymiarowej. Łatwo widać, że można to zrobić na $(q^{n+1}-q^2)(q^{n+1}-q^3) \ldots \ldots (q^{n+1}-q^s)$ sposobów (bazy traktujemy jako ciągi uporządkowane), jednak każda podprzestrzeń s-wymiarowa w $PG(n, q)$ odpowiada $(q^{s+1}-q^2)(q^{s+1}-q^3) \ldots (q^{s+1}-q^s)$ takim uzupełnieniom. Otrzymana konfiguracja ma zatem następujące parametry

$$v = \frac{q^{n+1}-1}{q-1}, \qquad k = \frac{q^{s+1}-1}{q-1},$$

$$\lambda = \frac{(q^{n+1}-q^2)(q^{n+1}-q^3) \ldots (q^{n+1}-q^s)}{(q^{s+1}-q^2)(q^{s+1}-q^3) \ldots (q^{s+1}-q^s)},$$

$$b = \frac{(q^{n+1}-1)(q^{n+1}-q) \ldots (q^{n+1}-q^s)}{(q^{s+1}-1)(q^{s+1}-q) \ldots (q^{s+1}-q^s)}, \tag{6.7}$$

$$r = \frac{(q^{n+1}-q)(q^{n+1}-q^2) \ldots (q^{n+1}-q^s)}{(q^{s+1}-q)(q^{s+1}-q^2) \ldots (q^{s+1}-q^s)}.$$

W zupełnie analogiczny sposób, przyjmując punkty i podprzestrzenie s-wymiarowe geometrii afinicznej $AG(n, q)$ jako punkty i bloki, otrzymujemy konfigurację o parametrach

$$v = q^n, \qquad k = q^s,$$

$$\lambda = \frac{(q^n-q)(q^n-q^2) \ldots (q^n-q^{s-1})}{(q^s-q)(q^s-q^2) \ldots (q^s-q^{s-1})},$$

$$b = \frac{q^n(q^n-1)(q^n-q) \ldots (q^n-q^{s-1})}{q^s(q^s-1)(q^s-q) \ldots (q^s-q^{s-1})}, \tag{6.8}$$

$$r = \frac{(q^n-1)(q^n-q) \ldots (q^n-q^{s-1})}{(q^s-1)(q^s-q) \ldots (q^s-q^{s-1})}.$$

Na zakończenie tego paragrafu zauważmy, że zbiór różnicowy $\{0, 1, 4, 14, 16\}$ mod 21 odpowiadający płaszczyźnie rzutowej $PG(2, 4)$ umożliwia nam rozwią-

zanie zagadnienia dotyczącego zawodów żużlowych opisanego we wstępie do tego rozdziału. Istotnie, konfiguracja resztowa uzyskana z tej płaszczyzny ma żądane parametry:

$$v^* = v-k = 21-5 = 16, \quad k^* = k-\lambda = 5-1 = 4,$$

$$\lambda^* = \lambda = 1, \quad b^* = b-1 = 21-1 = 20, \quad r^* = r = 5$$

(por. wzór (2.9). Możemy ją przedstawić następująco:

Biegi

Zawodnicy	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
1	*	*					*		*										*	
2		*	*					*		*										*
3	*			*	*					*		*								
4		*			*	*					*		*							
5			*			*	*					*		*						
6				*			*	*					*		*					
7					*			*	*					*		*				
8						*			*	*					*		*			
9							*			*	*					*		*		
10								*			*	*					*		*	
11									*			*	*					*		*
12	*										*			*	*					*
13	*		*										*			*	*			
14		*		*										*			*	*		
15			*		*										*			*	*	
16				*		*										*			*	*

§ 7. Dalsze przykłady zbiorów różnicowych

Znanych jest wiele nieskończonych rodzin zbiorów różnicowych; jedną z nich, złożoną z cyklicznych zbiorów różnicowych Singera poznaliśmy w poprzednim paragrafie. Oprócz paru wyjątków każdy znany zbiór różnicowy wpada do jednej z tych rodzin.

Opiszemy teraz pewną rodzinę zbiorów różnicowych w grupach addytywnych ciał Galois. Przypomnijmy, że element $a \in GF(q)$ nazywamy kwadratem, jeśli $a = b^2$ dla pewnego $b \in GF(q)$, $b \neq 0$.

TWIERDZENIE 7.1. *Jeśli p jest liczbą pierwszą oraz $p^m = 4t-1$, to kwadraty w $GF(p^m)$ tworzą zbiór różnicowy o parametrach*

(7.1) $$v = 4t-1, \quad k = 2t-1, \quad \lambda = t-1$$

w grupie addytywnej ciała $GF(p^m)$.

Dowód. Niech a, b będą dwoma różnymi kwadratami w $GF(p^m)$. Wobec twierdzenia 34 z Dodatku dokładnie jedna z różnic $a-b$, $b-a$ jest kwadratem. Bez zmniejszenia ogólności załóżmy, że tą różnicą jest $a-b=r$. Dla dowolnego kwadratu s elementy as, bs, rs są też kwadratami i spełniają równanie $as-bs=rs$, przy czym jeśli s przebiega wszystkie kwadraty w $GF(p^m)$, to rs również. Wynika stąd, że każdy kwadrat możemy otrzymać na tę samą liczbę sposobów jako różnicę kwadratów. Lecz każdej różnicy $a-b$ będącej kwadratem odpowiada różnica $b-a$ nie będąca kwadratem, a zatem dowolny element niezerowy możemy otrzymać na tę samą liczbę sposobów jako różnicę kwadratów. Oznacza to, że zbiór wszystkich kwadratów tworzy zbiór różnicowy o parametrach

$$v = p^m = 4t-1,$$
$$k = \tfrac{1}{2}(p^m-1) = \tfrac{1}{2}(4t-2) = 2t-1,$$
$$\lambda = k(k-1)/(v-1) = t-1. \quad \square$$

W przypadku gdy $m=1$, tzn. gdy $p \equiv 3 \pmod 4$, twierdzenie to orzeka, że reszty kwadratowe modulo p określają cykliczny zbiór różnicowy w $GF(p)$. Oczywiście tylko w takim przypadku otrzymany zbiór różnicowy jest cykliczny — dla $m>1$ grupa addytywna ciała $GF(p^m)$ nie jest cykliczna.

A oto przykłady zbiorów różnicowych typu opisanego w twierdzeniu 7.1:

$\{1, 2, 4\} \bmod 7$	$v=7,\ k=3,\ \lambda=1\ (t=2)$,
$\{1, 3, 4, 5, 9\} \bmod 11$	$v=11,\ k=5,\ \lambda=2\ (t=3)$,
$\{1, 4, 5, 6, 7, 9, 11, 16, 17\} \bmod 19$	$v=19,\ k=9,\ \lambda=4\ (t=5)$,
$\{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\} \bmod 23$	$v=32,\ k=11,\ \lambda=5\ (t=6)$,
kwadraty w $GF(3^3)$	$v=27,\ k=13,\ \lambda=6\ (t=7)$.

W tym ostatnim przypadku kwadraty najłatwiej wyznaczyć jako parzyste potęgi pewnego elementu pierwotnego w $GF(27)$.

Oczywiście twierdzenie 7.1 określa nieskończoną rodzinę zbiorów różnicowych, a nawet podrodzina złożona ze zbiorów cyklicznach jest nieskończona, gdyż z elementarnej teorii liczb wiadomo, że istnieje nieskończenie wiele liczb pierwszych $p \equiv 3 \pmod 4$.

Zbiory różnicowe o parametrach postaci (7.1) nazywamy *zbiorami różnicowymi Hadamarda*, dla przyczyn, które staną się jasne przy omawianiu macierzy Hadamarda (§ 10).

Znanych jest wiele innych typów zbiorów różnicowych. Większość z nich opiera się na pewnych teorioliczbowych własnościach reszt w $GF(p)$, lub ogólniej, na własnościach ciał $GF(p^m)$. Poniżej podajemy listę zawierającą niektóre z nich (p oznacza zawsze liczbę pierwszą, q potęgę liczby pierwszej).

Typ *S*. Zbiory różnicowe Singera

$$v = \frac{q^{n+1}-1}{q-1}, \quad k = \frac{q^n-1}{q-1}, \quad \lambda = \frac{q^{n-1}-1}{q-1}.$$

Typ Q. Kwadraty w $GF(q)$, $q \equiv 3 \pmod 4$)

$$v = q = 4t-1, \quad k = 2t-1, \quad \lambda = t-1.$$

Typ H_6. Niech $p = 4x^2+27$. Wówczas istnieje pierwiastek pierwotny r modulo p taki, że $\mathrm{Ind}_r(3) \equiv 1 \pmod 6$ (jeśli $a \equiv r^i \pmod p$, $0 \leqslant i < p$, to piszemy $i = \mathrm{Ind}_r(a)$). Te reszty $a \pmod p$, dla których $\mathrm{Ind}_r(a) \equiv 0$, 1 lub $3 \pmod 6$ tworzą zbiór różnicowy o parametrach

$$v = p = 4t-1, \quad k = 2t-1, \quad \lambda = t-1.$$

Typ T (liczby pierwsze bliźniacze). Jeśli p i $s = p+2$ są liczbami pierwszymi, r zaś pierwiastkiem pierwotnym zarówno dla p jak i dla s, to reszty $r^i \pmod{ps}$, $i = 1, 2, \ldots, \frac{1}{2}(p-1)(s-1)$ oraz reszty $0, s, 2s, \ldots, (p-1)s$ tworzą zbiór różnicowy o parametrach

$$v = ps = 4t-1, \quad k = 2t-1, \quad \lambda = t-1.$$

Typ B. Reszty dwukwadratowe modulo $p = 4x^2+1$, x nieparzyste (tzn. niezerowe czwarte potęgi w $GF(p)$)

$$v = p = 4x^2+1, \quad k = x^2, \quad \lambda = (x^2-1)/4.$$

Typ B_0. Reszty dwukwadratowe modulo $p = 4x^2+9$, x nieparzyste, wraz z zerem

$$v = p = 4x^2+9, \quad k = x^2+3, \quad \lambda = (x^2+3)/4.$$

Typ O. Reszty oktyczne modulo $p = 8a^2+1 = 64b^2+9$, gdzie a i b nieparzyste (tzn. niezerowe ósme potęgi w $GF(p)$)

$$v = p = 8a^2+1 = 64b^2+9, \quad k = a^2, \quad \lambda = b^2.$$

Typ O_0. Reszty oktyczne modulo $p = 8s^2+49 = 64b^2+441$, gdzie a nieparzyste i b parzyste

$$v = p = 8a^2+49 = 64b^2+441, \quad k = a^2+6, \quad \lambda = b^2+7.$$

Typ W_4. Niech $p \equiv 1 \pmod 4$ i $s = 3p+2$ będą liczbami pierwszymi. Załóżmy, że $ps = 1+4x$, gdzie x nieparzyste. Niech r będzie pierwiastkiem pierwotnym zarówno dla p jak i dla s, oraz niech $d = (p-1)(s-1)/4$. Wówczas reszty $1, r, r^2, \ldots, r^{d-1}, 0, s, 2s, \ldots, (p-1)s \pmod{ps}$ tworzą zbiór różnicowy o parametrach

$$v = ps, \quad k = (v-1)/4, \quad \lambda = (v-5)/16.$$

Pojęcie zbioru różnicowego można uogólniać na wiele sposobów. Oto jedno z takich uogólnień. *Rodziną różnicową* o parametrach v, k, λ, t w grupie G nazywamy rodzinę $(D_1, \ldots, D_t)$ podzbiorów k-elementowych tej grupy, taką, że każdy element $d \in G$ różny od jedynki można przedstawić na dokładnie λ sposobów w postaci

$$d = ab^{-1},$$

gdzie a, $b \in D_i$, $1 \leqslant i \leqslant t$. Łatwo widać (p. zad. 33), że taka rodzina różnicowa określa konfigurację $\langle G, \mathscr{B} \rangle$ o parametrach v, k, λ, jeśli przyjmiemy

$$\mathscr{B} = (D_i x\colon\ 1 \leqslant i \leqslant t \wedge x \in G). \tag{7.2}$$

Dla przykładu $(\{0, 2, 8\}, \{0, 3, 4\})$ jest rodziną różnicową o parametrach $v = 13$, $k = 3$, $\lambda = 1$, $t = 2$ w Z_{13}, określającą konfigurację:

$$\begin{array}{r} 0\\1\\2\\3\\4\\5\\6\\7\\8\\9\\10\\11\\12 \end{array}
\left[\begin{array}{ccccccccccccc:ccccccccccccc}
1&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0\\
0&1&0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0\\
1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&0&1&1\\
0&1&0&1&0&0&0&0&1&0&0&0&0&1&0&0&1&0&0&0&0&0&0&0&0&1\\
0&0&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&1&0&0&0&0&0&0&0&0\\
0&0&0&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&1&0&0&0&0&0&0\\
0&0&0&0&0&1&0&1&0&0&0&0&1&0&0&0&1&1&0&0&1&0&0&0&0&0\\
1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0&0\\
0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0&0\\
0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1&0&0\\
0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1&0\\
0&0&0&0&1&0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&0&1&1&0&0&1
\end{array}\right].$$

Taki sposób konstruowania konfiguracji odgrywa ważną rolę między innymi w dowodzie wspomnianego już twierdzenia Wilsona mówiącego, iż warunki (1.9), (1.10) są wystarczające dla istnienia konfiguracji dla dostatecznie dużego v.

§ 8. Mnożniki zbiorów różnicowych

Zaczniemy od prostego przykładu. Rozważmy konfigurację wyznaczoną przez zbiór różnicowy $\{0, 1, 3\} \bmod 7$. Wiemy, że ma ona regularną grupę automorfizmów, których działanie na zbiorze punktów jest postaci $x \mapsto (x+s) (\bmod 7)$. Okazuje się, że grupa ta nie wyczerpuje wszystkich automorfizmów. Przykładem dodatkowego automorfizmu jest $x \mapsto 2x (\bmod 7)$:

	B_0	B_1	B_2	B_3	B_4	B_5	B_6
0	1	0	0	0	1	0	1
1	1	1	0	0	0	1	0
2	0	1	1	0	0	0	1
3	1	0	1	1	0	0	0
4	0	1	0	1	1	0	0
5	0	0	1	0	1	1	0
6	0	0	0	1	0	1	1

	$2B_0 = B_6$	$2B_1 = B_1$	$2B_2 = B_3$	$2B_3 = B_5$	$2B_4 = B_0$	$2B_5 = B_2$	$2B_6 = B_4$
0	1	0	0	0	1	0	1
1	0	1	0	1	1	0	0
2	1	1	0	0	0	1	0
3	0	0	1	0	1	1	0
4	0	1	1	0	0	0	1
5	0	0	0	1	0	1	1
6	1	0	1	1	0	0	0

$x \mapsto 2x$

Ogólnie, niech D będzie dowolnym zbiorem różnicowym w addytywnej grupie przemiennej G rzędu v. Liczbę całkowitą t nazywamy *mnożnikiem* zbioru D, jeśli odwzorowanie $x \mapsto tx$ grupy G określa automorfizm konfiguracji wyznaczonej przez D (iloczyn liczby całkowitej przez element grupy definiujemy indukcyjnie: $0x = 0$, $(n+1)x = nx + x$, $-nx = n(-x)$).

Potrzebny nam będzie następujący elementarny fakt z teorii grup:

LEMAT 8.1. *Odwzorowanie $x \mapsto tx$ grupy przemiennej G rzędu v jest automorfizmem wtedy i tylko wtedy, gdy $(t, v) = 1$.*

Dowód. Nasze odwzorowanie zachowuje działanie grupowe, a więc jest automorfizmem wtedy i tylko wtedy, gdy nie istnieje element niezerowy x taki, że $tx = 0$. Niech r będzie rzędem elementu x i niech $tx = 0$. Z jednej strony mamy wtedy $r|t$ (por. Dodatek, lemat 16), z drugiej zaś $r|v$, gdyż rząd dowolnego elementu jest dzielnikiem rzędu grupy. Stąd wniosek, że $r|(t, v)$. Jeśli więc $(t, v) = 1$, to odwzorowanie $x \mapsto tx$ jest automorfizmem.

Wykażemy teraz, przez indukcję względem v, następujący pomocniczy fakt: Jeśli p jest liczbą pierwszą i $p|v$, to w każdej grupie przemiennej rzędu v istnieje element rzędu p. Jest to oczywiste dla $v = 1$, gdyż wtedy $p \nmid v$. Załóżmy, że jest to prawdą dla grup przemiennych rzędu mniejszego od v i niech x będzie dowolnym niezerowym elementem pewnej grupy G, $|G| = v$, $p|v$. Oznaczmy przez r rząd elementu x. Jeśli $p|r$, to $\frac{r}{p}x$ jest szukanym elementem, gdyż zgodnie z lematem 18 z Dodatku jego rząd wynosi $r/(r, r/p) = p$. Jeśli $p \nmid r$, to p dzieli $|G/H| = v/r < v$, gdzie H jest podgrupą cykliczną generowaną przez x. Na mocy założenia indukcyjnego istnieje element $[a] \in G/H$ rzędu p. Oznaczmy przez u rząd elementu a w grupie G. Wtedy $p|u$, gdyż łatwo widać, że

$$u = p \cdot (\text{rząd elementu } pa \text{ w grupie } H).$$

Zgodnie z lematem rząd elementu $\frac{u}{p}a$ równy jest p, co kończy dowód pomocniczego faktu.

Załóżmy teraz, że $(v, t) \neq 1$, tzn. że istnieje liczba pierwsza $p|(v, t)$. Istnieje wtedy w G element y rzędu p, dla którego mamy $ty = \frac{t}{p}py = \frac{t}{p}0 = 0$. Oznacza to, że odwzorowanie $x \mapsto tx$ nie jest automorfizmem grupy G. □

Jest oczywiste, iż na to, by automorfizm $x \mapsto tx$ grupy G określał automorfizm konfiguracji wyznaczonej przez D, potrzeba i wystarcza, aby zbiór tD był blokiem tej konfiguracji. A zatem t jest mnożnikiem wtedy i tylko wtedy, gdy $(t, v) = 1$ oraz

(8.1) $$tD = D + w$$

dla pewnego $w \in G$. Łatwo widać, że wszystkie mnożniki wyznaczają pewną grupę multyplikatywną reszt modulo v — podgrupę grupy multyplikatywnej wszystkich

reszt $r \pmod v$, $(r, v) = 1$. W przykładzie pokazanym na początku tego paragrafu grupa mnożników składa się z reszt 1, 2, 4 (mod 7).

W paragrafie tym udowodnimy pewne ogólne twierdzenie o istnieniu mnożników. Najpierw jednak podamy równoważne sformułowanie problemu w terminach pewnego pierścienia wyznaczonego przez grupę G. Będziemy rozważali formalne wielomiany postaci

$$\sum_{g \in G} c_g x^g,$$

gdzie współczynniki c_g są liczbami całkowitymi. W zbiorze tych wielomianów wprowadzamy działania $+$, $\cdot$ następująco:

$$\sum_{g \in G} c_g x^g + \sum_{g \in G} d_g x^g = \sum_{g \in G} (c_g + d_g) x^g,$$

$$\sum_{g \in G} c_g x^g \cdot \sum_{h \in G} c_h x^h = \sum_{g \in G} \sum_{h \in G} c_g c_h x^{g+h}.$$

Otrzymujemy w ten sposób pierścień, który będziemy oznaczali przez ZG. Piszemy zwykle c zamiast cx^0, oraz x^g zamiast $1x^g$. Odwzorowanie $g \mapsto x^g$ określa zanurzenie grupy G w grupę multyplikatywną pierścienia ZG. Dla dowolnego wielomianu $P(x) = \sum_{g \in G} c_g x^g \in ZG$ oraz liczby całkowitej t przez $P(x^t)$ będziemy rozumieli wielomian $\sum_{g \in G} c_g x^{tg}$.

Podzbiorowi $\{a_1, \ldots, a_k\} \subseteq G$ przyporządkowujemy wielomian

$$\Theta(x) = x^{a_1} + \ldots + x^{a_k},$$

zwany *wielomianem Halla*. Warunek na to, by zbiór $\{a_1, \ldots, a_k\}$ był zbiorem różnicowym, przyjmuje wtedy postać

$$\Theta(x) \cdot \Theta(x^{-1}) = n + \lambda T(x), \tag{8.2}$$

gdzie $n = k - \lambda$ oraz

$$T(x) = \sum_{g \in G} x^g.$$

Z kolei wzór (8.1) można zapisać jako

$$\Theta(x^t) = x^w \Theta(x).$$

A oto zapowiedziane twierdzenie o istnieniu mnożników:

TWIERDZENIE 8.2 (Hall i Ryser [1]). *Niech $D = \{a_1, \ldots, a_k\}$ będzie zbiorem różnicowym o parametrach v, k, λ w grupie przemiennej G, oraz niech p będzie liczbą pierwszą taką, że*

(i) $p \mid k - \lambda$,

(ii) $p \nmid v$,

(iii) $p > \lambda$.

Wówczas p jest mnożnikiem zbioru D.

Dowód. Zgodnie z poprzednimi uwagami mamy wykazać istnienie elementu $w \in G$ takiego, że $\Theta(x^p) = x^w \Theta(x)$. Obliczymy najpierw $[\Theta(x)]^p$. Korzystając z faktu, iż współczynnik dwumienny $\binom{p}{i}$ jest dla $i = 1, 2, \ldots, p-1$ wielokrotnością p, możemy napisać

$$[\Theta(x)]^p = x^{pa_1} + \ldots + x^{pa_k} + pW(x) = \Theta(x^p) + pW(x) \tag{8.3}$$

dla pewnego $W(x) \in ZG$. Mnożąc stronami (8.2) przez $[\Theta(x)]^{p-1}$ otrzymujemy

$$[\Theta(x)]^p \Theta(x^{-1}) = n[\Theta(x)]^{p-1} + \lambda[\Theta(x)]^{p-1} T(x). \tag{8.4}$$

Dla dowolnego $g \in G$ mamy oczywistą równość $x^g T(x) = T(x)$, a stąd $\Theta(x) T(x) = kT(x)$. Równość (8.4) przyjmuje więc postać

$$\begin{aligned} [\Theta(x)]^p \Theta(x^{-1}) &= n[\Theta(x)]^{p-1} + \lambda k^{p-1} T(x) \\ &= n[\Theta(x)]^{p-1} + \lambda(k^{p-1} - 1) T(x) + \lambda T(x). \end{aligned} \tag{8.5}$$

Założyliśmy, że p dzieli $n = k - \lambda$. Jeśli $p|k$, to p dzieli $\lambda = k - n$, jeśli zaś $p \nmid k$, to p dzieli $k^{p-1} - 1$ (por. Dodatek, wniosek 21). W obu przypadkach p dzieli $\lambda(k^{p-1} - 1)$. Zatem

$$[\Theta(x)]^p \Theta(x^{-1}) = pV(x) + \lambda T(x)$$

dla pewnego $V(x) \in ZG$. Uwzględniając (8.3) otrzymujemy stąd

$$\Theta(x^p) \Theta(x^{-1}) = pS(x) + \lambda T(x) \tag{8.6}$$

dla pewnego $S(x) \in ZG$. Lecz

$$\Theta(x^p) \Theta(x^{-1}) = \sum_{i=1}^{k} \sum_{j=1}^{k} x^{pa_i - a_j} = \sum_{g \in G} c_g x^g, \tag{8.7}$$

gdzie współczynniki c_g są nieujemne oraz

$$\sum_{g \in G} c_g = k^2. \tag{8.8}$$

Porównując (8.6) z (8.7) otrzymujemy

$$c_g \equiv \lambda \pmod{p}, \qquad g \in G.$$

Niech $S(x) = \sum_{g \in G} s_g x^g$. Wówczas

$$c_g = ps_g + \lambda, \tag{8.9}$$

a więc $s_g \geqslant 0$, gdyż $c_g \geqslant 0$, a założyliśmy $p > \lambda$. Ze wzorów (8.8), (8.9) wynika, że

$$k^2 = \sum_{g \in G} c_g = p \sum_{g \in G} s_g + v\lambda.$$

Lecz z równości $k(k-1) = \lambda(v-1)$ otrzymujemy $k^2 - \lambda v = k - \lambda = n$, a stąd

$$p \sum_{g \in G} s_g = n$$

oraz

(8.10)
$$pS(x)T(x) = p\Big(\sum_{g \in G} s_g\Big)T(x) = nT(x).$$

Przy zastosowaniu automorfizmu $g \mapsto pg$ grupy G obraz naszego zbioru różnicowego pozostaje zbiorem różnicowym, a zatem równanie (8.2) przechodzi na

(8.11)
$$\Theta(x^p)\Theta(x^{-p}) = n + \lambda T(x).$$

Podobnie, stosując automorfizm $g \mapsto -g$ do wzoru (8.6) otrzymujemy

(8.12)
$$\Theta(x^{-p})\Theta(x) = pS^*(x) + \lambda T(x),$$

gdzie $S^*(x) = \sum_{g \in G} s_g x^{-g}$. Zauważmy teraz, że iloczyn lewych stron równości (8.2) i (8.11) jest taki sam jak iloczyn lewych stron równości (8.6) i (8.12). Porównanie odpowiednich iloczynów prawych stron daje

$$\big(pS(x) + \lambda T(x)\big)\big(pS^*(x) + \lambda T(x)\big) = \big(n + \lambda T(x)\big)^2.$$

Korzystając z równości $pS(x)T(x) = nT(x)$, $pS^*(x)T(x) = nT(x)$ (por. (8.10)) otrzymujemy

$$p^2 S(x) S^*(x) = n^2,$$

czyli

(8.13)
$$p^2 \sum_{g \in G} s_g x^g \sum_{h \in G} s_h x^{-h} = n^2.$$

Przypomnijmy, że wykazaliśmy już, iż współczynniki s_g są nieujemne. Stąd wniosek, że tylko jeden spośród tych współczynników jest niezerowy. Istotnie, dwa takie współczynniki s_g, s_h dawałyby niezerowy współczynnik przy x^{g-h}, gdzie $g - h \neq 0$, wbrew temu, że po prawej stronie wzoru (8.13) jedynie współczynnik przy x^0 jest niezerowy. Tak więc $S(x)$ jest postaci $c_w x^w$ dla pewnego $w \in G$, i wobec (8.13) mamy

$$pS(x) = nx^w.$$

Podstawiając to wyrażenie na $pS(x)$ do (8.6) otrzymujemy równość

$$\Theta(x^p)\Theta(x^{-1}) = nx^w + \lambda T(x),$$

która po pomnożeniu stronami przez $\Theta(x)$ i skorzystaniu z (8.2) przyjmuje postać

$$\Theta(x^p)\big(n + \lambda T(x)\big) = nx^w \Theta(x) + \lambda \Theta(x) T(x).$$

Uwzględniając fakt, że $\Theta(x^p)T(x) = \Theta(x)T(x) = kT(x)$ otrzymujemy ostatecznie

$$n\Theta(x^p) + \lambda k T(x) = nx^w \Theta(x) + \lambda k T(x),$$

czyli

$$\Theta(x^p) = x^w \Theta(x),$$

co kończy dowód. □

Warto tu wspomnieć, że nie jest znany przykład, który by wskazywał, że warunek $p > \lambda$ w założeniach twierdzenia 8.2 jest istotny.

Każdy mnożnik zbioru różnicowego $D \subseteq G$ ustala element zerowy grupy G, i tylko ten element, a więc na mocy lematu 5.2 ustala dokładnie jeden blok konfiguracji wyznaczonej przez D. Bardzo ważne w zastosowaniach jest następujące uogólnienie tej obserwacji:

TWIERDZENIE 8.3. *Niech D będzie zbiorem różnicowym o parametrach v, k, λ w grupie przemiennej G. Wówczas każdy mnożnik zbioru D ustala dokładnie jeden blok konfiguracji wyznaczonej przez D. Jeśli $(v, k) = 1$, to każdy mnożnik ustala ten sam blok.*

Dowód. Niech $D = \{a_1, \ldots, a_k\}$, $b = a_1 + \ldots + a_k$. Dla dowolnego $x \in G$ mamy $(a_1 + x) + \ldots + (a_k + x) = b + kx$. Jeśli $(k, v) = 1$, to na mocy lematu 8.1 istnieje dokładnie jeden element x taki, że $b + kx = 0$. Blok $D + x$ jest ustalony przez każdy mnożnik, gdyż jeśli $t(D+x) = D+y$, to $b+ky = t(b+kx) = 0$, czyli $y = x$. □

Klasycznym zastosowaniem teorii mnożników jest dowód następującego faktu:

TWIERDZENIE 8.4. *Nie istnieje cykliczna płaszczyzna rzutowa rzędu* 10.

Dowód. Mamy $v = 111$, $k = 11$, $\lambda = 1$, $n = 10$. Załóżmy, że istnieje zbiór różnicowy $D \subseteq \boldsymbol{Z}_{111}$ o tych parametrach. Wtedy zgodnie z twierdzeniem 8.2 liczby 2 i 5 są mnożnikami. Lecz $(111, 11) = 1$, zatem istnieje blok $B = D + x$ ustalony przez oba te mnożniki. Jeśli $c \in B$, to również $2c, 4c, 5c \in B$. Z równości $2c - c = 5c - 4c$ i tego, że $\lambda = 1$ wnioskujemy, iż $2c = 5c$ i $c = 4c$, tzn. $3c = 0$. Równość ta powinna być prawdziwa dla każdego spośród jedenastu elementów $c \in B$, podczas gdy w $\boldsymbol{Z}_{111}$ istnieją tylko 3 takie elementy: 0, 37 i 74. Otrzymana sprzeczność dowodzi twierdzenia. □

Twierdzenie 8.2 może również służyć do konstrukcji pewnych zbiorów różnicowych. Niech na przykład $v = 37$, $k = 9$, $\lambda = 2$. Wówczas $n = 9 - 2 = 7$ i jeśli zbiór różnicowy o tych parametrach istnieje, to 7 jest jego mnożnikiem. Niech $c \neq 0$ będzie elementem bloku ustalonego przez ten mnożnik. Wówczas blok ten zawiera elementy $c, 7c, 7^2c, \ldots, 7^8c \pmod{37}$. Możemy przyjąć, że $c = 1$, gdyż $x \mapsto dx$, dla $cd \equiv 1 \pmod{37}$, jest automorfizmem grupy $\boldsymbol{Z}_{37}$ przeprowadzającym c na 1. Otrzymujemy zatem

$$\{1, 7, \ldots, 7^8\} \bmod 37 = \{1, 7, 9, 10, 12, 16, 26, 33, 34\} \bmod 37$$

jako podzbiór szukanego zbioru różnicowego. Można łatwo sprawdzić, że w istocie jest to właśnie zbiór różnicowy o parametrach $v = 37$, $k = 9$, $\lambda = 2$. Ważną cechą tej konstrukcji jest fakt, że dowodzi ona zarazem, iż cykliczny zbiór

różnicowy o danych parametrach jest jedyny z dokładnością do równoważności. Można w ten sposób dowieść jedyności wielu znanych cyklicznych zbiorów różnicowych.

Oprócz twierdzenia 8.2 znane są również inne warunki dostateczne istnienia mnożników (p. M. Hall [3]). Nie jest jednak znany taki, o którym byłoby wiadomo, że jest konieczny. Warto tu wspomnieć, że twierdzenie 8.2 gwarantuje istnienie nietrywialnego mnożnika (tzn. mnożnika $t \not\equiv 1 \pmod v$) dla wszystkich znanych cyklicznych zbiorów różnicowych. Z kolei łatwo podać przykład niecyklicznego zbioru różnicowego bez nietrywialnego mnożnika. Takim zbiorem jest na przykład rozważany już zbiór

(8.14) $$D = \{0000,\ 0001,\ 0010,\ 0100,\ 1000,\ 1111\}$$

w grupie $G = \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2$. Wynika to po prostu z faktu, iż w grupie tej $tx = 0$, gdy t parzyste, i $tx = x$, gdy t nieparzyste. Nie oznacza to bynajmniej, iż konfiguracja wyznaczona przez ten zbiór nie ma innych automorfizmów oprócz wyznaczonych przez translacje grupy G postaci $x \mapsto x+g$, $g \in G$ (p. zad. 42).

§ 9. Ortogonalne kwadraty łacińskie

Z kwadratami łacińskimi spotkaliśmy się już w rozdziale 4 (p. § 7). Przypomnijmy że przez kwadrat łaciński rzędu n rozumiemy macierz wymiaru $n \times n$ o elementach ze zbioru $\{1, \ldots, n\}$, która zawiera każdy element tego zbioru dokładnie raz w każdym wierszu i dokładnie raz w każdej kolumnie (zamiast $\{1, \ldots, n\}$ możemy oczywiście rozważać dowolny inny zbiór n-elementowy). Obecnie zajmiemy się zagadnieniami związanymi z pojęciem ortogonalności kwadratów łacińskich. Będziemy mówili, że dwie macierze $A = [a_{ij}]$, $B = [b_{ij}]$ wymiaru $n \times n$ o elementach ze zbioru $N = \{1, \ldots, n\}$ są *ortogonalne* — piszemy wtedy $A \perp B$ — jeśli wszystkie spośród n^2 par $\langle a_{ij}, b_{ij} \rangle$, $1 \leqslant i \leqslant n$, $1 \leqslant j \leqslant n$, są różne, tzn. jeśli

$$\{\langle a_{ij}, b_{ij} \rangle : 1 \leqslant i \leqslant n \wedge 1 \leqslant j \leqslant n\} = N \times N.$$

Przykładem macierzy ortogonalnych rzędu n są macierze R, C przedstawione poniżej:

$$R = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 2 & 2 & \ldots & 2 \\ \cdots & \cdots & \cdots & \cdots \\ n & n & \ldots & n \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 2 & \ldots & n \\ 1 & 2 & \ldots & n \\ \cdots & \cdots & \cdots & \cdots \\ 1 & 2 & \ldots & n \end{bmatrix}.$$

Macierze te mają tę ciekawą własność, iż pozwalają zdefiniować pojęcie kwadratu łacińskiego w terminach ortogonalności: Macierz L wymiaru $n \times n$ o elementach z $\{1, \ldots, n\}$ jest kwadratem łacińskim wtedy i tylko wtedy, gdy $L \perp R$ i $L \perp C$.

Będziemy mówili, że $\{L_1, \ldots, L_t\}$ jest *zbiorem ortogonalnych kwadratów łaciń-*

skich, jeśli $L_i \perp L_j$ dla dowolnych $i \neq j$, $1 \leqslant i, j \leqslant t$. Oto na przykład zbiór trzech ortogonalnych kwadratów łacińskich rzędu 4:

$$L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{bmatrix}, \quad L_3 = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \\ 2 & 1 & 4 & 3 \end{bmatrix}.$$

Wiele ciekawych problemów związanych jest z wielkością $N(n)$, zdefiniowaną jako maksymalna liczność zbioru ortogonalnych kwadratów łacińskich rzędu n. Mamy oczywiście $N(1) = 1$, $N(2) = 1$, gdyż jedynymi kwadratami łacińskimi rzędu 2 są

$$L_1 = \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

które nie są ortogonalne.

TWIERDZENIE 9.1. *$N(n) \leqslant n-1$ dla każdego $n \geqslant 2$.*

Dowód. Niech $L_1 = [a_{ij}^{(1)}], \ldots, L_t = [a_{ij}^{(t)}]$ określają zbiór t ortogonalnych kwadratów łacińskich rzędu n. Własność ortogonalności zostanie zachowana, jeśli dokonamy zamiany nazw elementów w pewnym kwadracie zgodnie z dowolną permutacją φ zbioru $\{1, \ldots, n\}$, tzn. jeśli zastąpimy $[a_{ij}^{(k)}]$ przez $[\varphi(a_{ij}^{(k)})]$. Możemy zatem zakładać, że

$$\begin{aligned} a_{11}^{(1)} &= a_{11}^{(2)} = \ldots = a_{11}^{(t)} = 1, \\ a_{12}^{(1)} &= a_{12}^{(2)} = \ldots = a_{12}^{(t)} = 2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{1n}^{(1)} &= a_{1n}^{(2)} = \ldots = a_{1n}^{(t)} = n. \end{aligned}$$

Rozważmy teraz elementy

$$a_{21}^{(1)}, a_{21}^{(2)}, \ldots, a_{21}^{(t)}. \tag{9.1}$$

Żaden z nich nie może być równy 1, gdyż naruszałoby to warunek, iż $L_1, \ldots, L_t$ są kwadratami łacińskimi. Żadne dwa spośród elementów (9.1) nie są równe, gdyż naruszałoby to z kolei własność ortogonalności. Tak więc $t \leqslant n-1$. □

Okazuje się, że nierówność w twierdzeniu 9.1 jest osiągana wtedy i tylko wtedy, gdy istnieje płaszczyzna rzutowa rzędu n. Zanim to udowodnimy, uczyńmy najpierw parę pomocniczych uwag. Zauważmy przede wszystkim, że w definicji ortogonalności kształt macierzy jest nieistotny. Ważne jest jedynie to, by był ten sam dla obu macierzy, tak aby można je było na siebie „nałożyć” i sprawdzić, czy otrzymujemy wszystkie możliwe pary elementów. Oczywiście $L_1, \ldots, L_t$ tworzą zbiór ortogonalnych kwadratów łacińskich wtedy i tylko wtedy, gdy macierze R, C, $L_1, \ldots, L_t$ są parami ortogonalne. Jeśli teraz zastąpimy każdą z tych macierzy

przez jeden wiersz długości n^2 zawierający kolejno wszystkie wiersze tej macierzy, to otrzymamy pewną macierz o $s = t+2$ wierszach i n^2 kolumnach. Na przykład pokazany poprzednio zbiór trzech ortogonalnych kwadratów łacińskich rzędu 4 prowadzi do następującej macierzy:

$$\begin{bmatrix} 1&1&1&1&2&2&2&2&3&3&3&3&4&4&4&4 \\ 1&2&3&4&1&2&3&4&1&2&3&4&1&2&3&4 \\ 1&2&3&4&4&3&2&1&2&1&4&3&3&4&1&2 \\ 1&2&3&4&2&1&4&3&3&4&1&2&4&3&2&1 \\ 1&2&3&4&3&4&1&2&4&3&2&1&2&1&4&3 \end{bmatrix}.$$

Macierz ta – oznaczmy ją przez $[c_{ij}]$ – ma tę własność, że jej dowolne dwa wiersze są ortogonalne, tj. dla dowolnych i, j, gdzie $1 \leqslant i < j \leqslant s$, wszystkie pary $\langle c_{ir}, c_{jr} \rangle$, $1 \leqslant r \leqslant n^2$, są różne.* Macierz o tej własności będziemy nazywali *tablicą ortogonalną*. Na odwrót, z dowolnej tablicy ortogonalnej wymiaru $s \times n^2$ możemy otrzymać zbiór $s-2$ ortogonalnych kwadratów łacińskich rzędu n. W tym celu dokonujemy najpierw takiej permutacji kolumn naszej tablicy, by pary elementów określone przez dwa pierwsze wiersze były uporządkowane leksykograficznie, tzn. by wiersze te były postaci

$$\begin{bmatrix} 1 & 1 & \dots & 1 & 2 & 2 & \dots & 2 & \dots & n & n & \dots & n \\ 1 & 2 & \dots & n & 1 & 2 & \dots & n & \dots & 1 & 2 & \dots & n \end{bmatrix}$$

– taką tablicę ortogonalną będziemy nazywali *znormalizowaną*. Łatwo widać, że pozostałe $s-2$ wiersze określają wtedy $s-2$ ortogonalne kwadraty łacińskie. Każdy taki kwadrat otrzymujemy dzieląc pewien wiersz na n odcinków długości n i traktując każdy z odcinków jako wiersz kwadratu. □

TWIERDZENIE 9.2. *Zbiór $n-1$ ortogonalnych kwadratów łacińskich rzędu n istnieje wtedy i tylko wtedy, gdy istnieje płaszczyzna rzutowa rzędu n.*

Dowód. Pokażemy najpierw jak skonstruować zbiór ortogonalnych kwadratów łacińskich mając daną płaszczyznę rzutową. Ustalmy pewną prostą L naszej płaszczyzny. Niech $p_1, \dots, p_{n+1}$ będą punktami na tej prostej, oraz niech $q_1, \dots, q_{n^2}$ będą pozostałymi punktami. Dla każdego punktu p_j, $1 \leqslant j \leqslant n+1$, ponumerujmy w dowolny sposób n prostych różnych od L przechodzących przez p_j liczbami $1, 2, \dots, n$. Określmy macierz $A = [a_{ij}]$ o $n+1$ wierszach i n^2 kolumnach następująco: a_{ij} jest liczbą przyporządkowaną prostej przechodzącej przez p_i i q_j. Wykażemy, że A jest tablicą ortogonalną. Istotnie, załóżmy, że $\langle a_{ij}, a_{i'j} \rangle = \langle a_{ik}, a_{i'k} \rangle$, $i' \neq i$. Oznacza to, że zarówno q_j jak i q_k leżą na przecięciu prostej przechodzącej przez p_i oznaczonej liczbą a_{ij} oraz prostej przechodzącej przez $p_{i'}$, oznaczonej liczbą $a_{i'j}$. Proste te są oczywiście różne, stąd $q_j = q_k$, tzn.

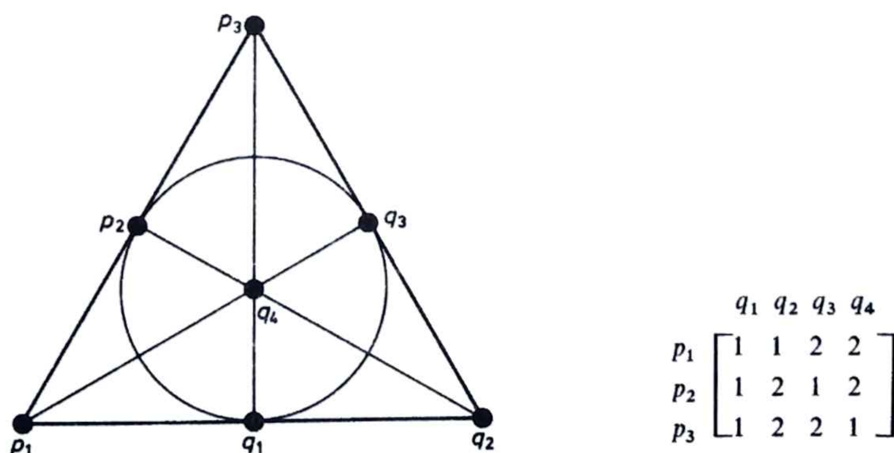
* Oczywiście nie należy mylić tego pojęcia ortogonalności z ortogonalnością w sensie zerowego iloczynu skalarnego.

$j = k$. Tak więc A jest tablicą ortogonalną wymiaru $(n+1) \times n^2$, która określa – w myśl naszych poprzednich uwag – zbiór $n-1$ ortogonalnych kwadratów łacińskich rzędu n.

Konstrukcja płaszczyzny rzutowej rzędu n z dowolnej tablicy ortogonalnej $A = [a_{ij}]$ wymiaru $(n+1) \times n^2$ przebiega podobnie. Przyporządkowujemy kolumnom n^2 punktów $q_1, \ldots, q_{n^2}$, oraz rozważamy dodatkowych $n+1$ punktów $p_1, \ldots, p_{n+1}$. Dla $1 \leqslant i \leqslant n+1$, $1 \leqslant j \leqslant n$, tworzymy $(n+1)n = n^2+n$ prostych L_{ij} składających się z punktu p_i oraz punktów q_k takich, że $a_{ik} = j$. Dodatkowo określamy prostą L składającą się z punktów $p_1, \ldots, p_{n+1}$. Każda prosta L_{ij} ma dokładnie jeden punkt wspólny z L, mianowicie punkt p_i. Podobnie dwie różne proste L_{ij}, $L_{ij'}$ mają jedyny punkt wspólny p_i. Dwie proste L_{ij}, $L_{i'j'}$, $i' \neq i$, $j' \neq j$, przecinają się również w dokładnie jednym punkcie, mianowicie w punkcie q_k takim, że $a_{ik} = j$, $a_{i'k} = j'$. Zgodnie z naszą konstrukcją każda prosta zawiera dokładnie $n+1$ punktów. Na mocy twierdzenia 3.1 określone przez nas proste tworzą konfigurację kwadratową o parametrach $v = n^2+n+1$, $k = n+1$, $\lambda = 1$, czyli – wobec twierdzenia 2.2 – płaszczyznę rzutową rzędu n. □

Warto zauważyć, że w naszej konstrukcji każdy wiersz tablicy ortogonalnej odpowiada wiązce n prostych równoległych w płaszczyźnie afinicznej otrzymanej z płaszczyzny rzutowej przez usunięcie prostej złożonej z „punktów w nieskończoności" $p_1, \ldots, p_{n+1}$ (por. rozdz. 1, § 12).

Odpowiedniość między tablicą ortogonalną wymiaru 3×2^2 powstałą z kwadratu łacińskiego $\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}$ oraz płaszczyzną rzutową rzędu 2 przedstawiono na rys. 32.



Rys. 32. Odpowiedniość między tablicą ortogonalną wymiaru $(n+1) \times n^2$ a płaszczyzną rzutową rzędu n w przypadku $n = 2$

Wiemy, że jeśli n jest potęgą liczby pierwszej, to istnieje płaszczyzna rzutowa rzędu n. Otrzymujemy stąd następujący wniosek:

WNIOSEK 9.3. *Jeśli $n = p^m$, gdzie p jest liczbą pierwszą i $m \geqslant 1$, to $N(n) = n-1$.*

Pokażemy teraz prostą konstrukcję zbioru $n-1$ ortogonalnych kwadratów łacińskich rzędu $n = p^m$ nie korzystającą z istnienia płaszczyzny rzutowej rzędu n. Oznaczmy w tym celu elementy ciała $GF(p^m)$ przez $a_0 = 0$, $a_1 = 1$, $a_2, \ldots, a_{n-1}$, oraz określmy $n-1$ macierzy kwadratowych

$$L_k = [a_{ij}^{(k)}], \quad 1 \leqslant k \leqslant n-1, \tag{9.2}$$

wymiaru $n \times n$ następująco:

$$a_{ij}^{(k)} = a_k a_i + a_j.$$

Każda z macierzy L_k jest kwadratem łacińskim (ściśle rzecz biorąc, po utożsamieniu każdego elementu a_i z liczbą $i+1$). Istotnie, jeśli $a_{ij}^{(k)} = a_{ij'}^{(k)}$, tzn. jeśli

$$a_k a_i + a_j = a_k a_i + a_{j'},$$

to $a_j = a_{j'}$, czyli $j = j'$. Podobnie z

$$a_k a_i + a_j = a_k a_{i'} + a_j$$

wnioskujemy, że $i = i'$, bowiem $a_k \neq 0$. Wykażemy teraz, że kwadraty (9.2) są ortogonalne. Przypuśćmy w tym celu, że $\langle a_{ij}^{(k)}, a_{ij}^{(l)} \rangle = \langle a_{i'j'}^{(k)}, a_{i'j'}^{(l)} \rangle$, $1 \leqslant k < l \leqslant n-1$. Mamy wtedy

$$\begin{aligned} a_k a_i + a_j &= a_k a_{i'} + a_{j'}, \\ a_l a_i + a_j &= a_l a_{i'} + a_{j'}. \end{aligned} \tag{9.3}$$

Odejmując stronami te równości otrzymujemy

$$(a_k - a_l) a_i = (a_k - a_l) a_{i'},$$

a stąd $i = i'$, jako że $a_k - a_l \neq 0$. Równość (9.3) możemy więc zapisać jako

$$a_k a_i + a_j = a_k a_i + a_{j'},$$

co dowodzi, że $j = j'$. Tak więc $L_1, \ldots, L_{n-1}$ jest zbiorem ortogonalnych kwadratów łacińskich rzędu n.

Oczywiście podana tu konstrukcja jest – wobec twierdzenia 9.2 – niezależnym dowodem istnienia płaszczyzn rzutowych rzędu będącego potęgą liczby pierwszej.

Zajmiemy się teraz wartością $N(n)$ dla dowolnego n. Ważną rolę odgrywać będzie następujące twierdzenie.

TWIERDZENIE 9.4 (MacNeish [1]). *Jeśli istnieje zbiór t ortogonalnych kwadratów łacińskich rzędu n oraz zbiór t ortogonalnych kwadratów łacińskich rzędu m, to istnieje zbiór t ortogonalnych kwadratów łacińskich rzędu nm.*

Dowód. Niech $A_k = [a_{ij}^{(k)}]$, $1 \leqslant k \leqslant t$ będą ortogonalnymi kwadratami łaciń-

skimi rzędu n, zaś $B_k = [b_{ij}^{(k)}]$, $1 \leqslant k \leqslant t$, ortogonalnymi kwadratami łacińskimi rzędu m. Określamy macierze L_k, $1 \leqslant k \leqslant t$, wymiaru $nm \times nm$ następująco:

$$L_k = \begin{bmatrix} \langle a_{11}^{(k)}, B_k \rangle & \langle a_{12}^{(k)}, B_k \rangle & \dots & \langle a_{1n}^{(k)}, B_k \rangle \\ \langle a_{21}^{(k)}, B_k \rangle & \langle a_{22}^{(k)}, B_k \rangle & \dots & \langle a_{2n}^{(k)}, B_k \rangle \\ \dots & \dots & \dots & \dots \\ \langle a_{n1}^{(k)}, B_k \rangle & \langle a_{n2}^{(k)}, B_k \rangle & \dots & \langle a_{nn}^{(k)}, B_k \rangle \end{bmatrix}.$$

Przez $\langle a_{ij}^{(k)}, B_k \rangle$ oznaczamy tu podmacierz $[c_{pq}]$ wymiaru $m \times m$ taką, że c_{pq} jest parą $\langle a_{ij}^{(k)}, b_{pq}^{(k)} \rangle$. Macierze L_k są kwadratami łacińskimi rzędu nm (jeśli ponumerujemy wszystkie pary $\langle a, b \rangle$, $1 \leqslant a \leqslant n$, $1 \leqslant b \leqslant m$, liczbami od 1 do nm). Istotnie, dowolne dwie pary w pewnym wierszu lub pewnej kolumnie macierzy L_k różnią się albo na pierwszej albo na drugiej współrzędnej. Aby wykazać, że $L_1, \dots, L_t$ tworzą zbiór ortogonalnych kwadratów łacińskich, załóżmy, że

$$\langle \langle a_{ij}^{(k)}, b_{pq}^{(k)} \rangle, \langle a_{ij}^{(l)}, b_{pq}^{(l)} \rangle \rangle = \langle \langle a_{i'j'}^{(k)}, b_{p'q'}^{(k)} \rangle, \langle a_{i'j'}^{(l)}, b_{p'q'}^{(l)} \rangle \rangle,$$

$1 \leqslant k < l \leqslant t$. Wtedy w szczególności

$$a_{ij}^{(k)} = a_{i'j'}^{(k)}, \qquad a_{ij}^{(l)} = a_{i'j'}^{(l)}.$$

Lecz wobec ortogonalności kwadratów A_k, A_l oznacza to, iż $i = i'$, $j = j'$. Podobnie z ortogonalności kwadratów B_k, B_l wnioskujemy, że $p = p'$ i $q = q'$. Tak więc $L_k \perp L_l$. □

Z twierdzenia 9.4 otrzymujemy jako wniosek następujące dolne oszacowanie liczb $N(n)$.

TWIERDZENIE 9.5. *Niech $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ będzie rozkładem kanonicznym liczby n na czynniki pierwsze, i niech*

$$t = \min_{1 \leqslant i \leqslant k} (p_i^{\alpha_i} - 1).$$

Wówczas istnieje zbiór t ortogonalnych kwadratów łacińskich rzędu n.

Dowód. Zgodnie z wnioskiem 9.3 istnieje dla $i = 1, 2, \dots, k$ zbiór t kwadratów łacińskich rzędu $p_i^{\alpha_i}$. Wystarczy teraz $(k-1)$-krotnie zastosować twierdzenie 9.4. □

Twierdzenie 9.5 gwarantuje istnienie pary ortogonalnych kwadratów łacińskich rzędu n dla dowolnego $n > 1$, jeśli tylko $n \not\equiv 2 \pmod 4$.

Przypadek $n \equiv 2 \pmod 4$ ma bardzo ciekawą historię. Wiąże się on z następującym „problemem 36 oficerów” zaproponowanym przez Eulera: Danych jest 36 oficerów sześciu różnych rang z sześciu pułków, po sześciu oficerów różnych rang z każdego pułku. Czy można ich ustawić w czworobok wymiaru 6×6 tak, by w każdym rzędzie i każdej kolumnie każda ranga i każdy pułk były reprezentowane dokładnie raz? Istnienie takiego ustawienia jest równoważne istnieniu pary ortogonalnych kwadratów łacińskich rzędu 6. Istotnie, w szukanym ustawieniu rangi

określają jeden kwadrat łaciński, a pułki drugi. Kwadraty te są ortogonalne, gdyż założyliśmy, że wśród oficerów każda kombinacja ranga–pułk występuje dokładnie raz. Euler był przekonany, że problem ten nie ma rozwiązania. Co więcej, w 1782 r. wysunął on przypuszczenie, że nie istnieje para ortogonalnych kwadratów łacińskich rzędu n dla żadnego $n \equiv 2 (\mathrm{mod}\, 4)$. Jak już zauważyliśmy, jest to oczywiście prawdą dla $n = 2$. Około roku 1900 G. Tarry [1] potwierdził prawdziwość przypuszczenia Eulera dla $n = 6$ przez systematyczne sprawdzenie wszystkich możliwości (zauważmy przy okazji, że stanowi to dowód nieistnienia płaszczyzny rzutowej rzędu 6). Okazało się jednak, że są to jedyne dwa przypadki, w których przypuszczenie Eulera jest prawdziwe: w roku 1959 R. C. Bose, S. S. Shrikhande i E. T. Parker [1] wykazali, że dla dowolnego $n > 6$ istnieje para ortogonalnych kwadratów łacińskich rzędu n. Przypadek $n \equiv 2 (\mathrm{mod}\, 4)$ okazał się zresztą pechowy nie tylko dla Eulera. W roku 1922 H. F. MacNeish opublikował błędny dowód równości $N(n) = \min_{1 \leqslant i \leqslant k} (p_i^{\alpha_i} - 1)$ (oznaczenia takie jak w twierdzeniu 9.5), z której wynika oczywiście prawdziwość przypuszczenia Eulera.

Konstrukcja pary ortogonalnych kwadratów łacińskich rzędu n dla dowolnego $n \equiv 2 (\mathrm{mod}\, 4)$ jest dość skomplikowana, pokażemy ją więc jedynie dla szczególnego przypadku $n \equiv 10 (\mathrm{mod}\, 12)$. Kluczowe znaczenie mieć będzie następujący lemat pochodzący od Bose'a, Shrikhande i Parkera [1].

LEMAT 9.6. *Jeśli istnieje para ortogonalnych kwadratów łacińskich rzędu m, to istnieje para ortogonalnych kwadratów łacińskich rzędu $3m+1$.*

Dowód. Istnienie pary ortogonalnych kwadratów łacińskich rzędu m jest równoważne istnieniu tablicy ortogonalnej T wymiaru $4 \times m^2$. Aby udowodnić twierdzenie, wystarczy pokazać, jak z takiej tablicy otrzymać tablicę ortogonalną S wymiaru $4 \times (3m+1)^2$. W tym celu utwórzmy dla $i = 0, 1, \ldots, 2m$ następujące ciągi długości m:

$$A_i = \langle i, i, \ldots, i \rangle,$$
$$B_i = \langle i+1, i+2, \ldots, i+m \rangle,$$
$$C_i = \langle i-1, i-2, \ldots, i-m \rangle,$$

których elementy są obliczane modulo $2m+1$, oraz przyjmijmy

$$X_i = \langle 2m+1, 2m+2, \ldots, 3m \rangle.$$

Utwórzmy następujące ciągi długości $m(2m+1)$:

$$A = \langle A_0, A_1, \ldots, A_{2m} \rangle,$$
$$B = \langle B_0, B_1, \ldots, B_{2m} \rangle,$$
$$C = \langle C_0, C_1, \ldots, C_{2m} \rangle,$$
$$X = \langle X_0, X_1, \ldots, X_{2m} \rangle.$$

Jeśli założymy, że elementy tablicy T są ze zbioru $\{2m+1, 2m+2, \ldots, 3m\}$, to macierz

$$S = \left[\underbrace{\begin{matrix} A & B & C & X \\ B & A & X & C \\ C & X & A & B \\ X & C & B & A \end{matrix}}_{4m(2m+1)} \vdots \underbrace{\quad T \quad}_{m^2} \vdots \underbrace{\begin{matrix} 0 & 1 & \ldots & 2m \\ 0 & 1 & \ldots & 2m \\ 0 & 1 & \ldots & 2m \\ 0 & 1 & \ldots & 2m \end{matrix}}_{2m+1}\right]$$

jest tablicą ortogonalną o czterech wierszach, $4m(2m+1)+m^2+2m+1 = 9m^2+6m+1 = (3m+1)^2$ kolumnach i elementach ze zbioru $\{0, 1, \ldots, 3m\}$. Aby się o tym łatwo przekonać, zbadajmy dwa pierwsze wiersze tej macierzy. Łatwo można sprawdzić, że kolumny podmacierzy

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}$$

wyczerpują wszystkie pary $\begin{bmatrix} i \\ j \end{bmatrix}$, $0 \leqslant i, j \leqslant 2m$, $i \neq j$. Z kolei kolumny podmacierzy

$$\begin{bmatrix} C & X \\ X & C \end{bmatrix}$$

wyczerpują wszystkie pary $\begin{bmatrix} i \\ j \end{bmatrix}$, $\begin{bmatrix} j \\ i \end{bmatrix}$, $0 \leqslant i \leqslant 2m$, $2m+1 \leqslant j \leqslant 3m$. Z definicji macierzy T jej dwa pierwsze wiersze zawierają wszystkie kolumny postaci $\begin{bmatrix} i \\ j \end{bmatrix}$, $2m+1 \leqslant i, j \leqslant 3m$. Pozostałe kolumny dwóch pierwszych wierszy zawierają wszystkie pary $\begin{bmatrix} i \\ i \end{bmatrix}$, $0 \leqslant i \leqslant 2m$. W sumie otrzymaliśmy wszystkie możliwe pary $\begin{bmatrix} i \\ j \end{bmatrix}$, $0 \leqslant i, j \leqslant 3m$.

Podobne rozumowanie można zastosować dla dowolnych dwóch wierszy macierzy S. Istotne jest to, że każde dwa wiersze zawierają jedną z następujących trzech podmacierzy

$$\begin{bmatrix} A & B \\ B & A \end{bmatrix}, \quad \begin{bmatrix} B & C \\ C & B \end{bmatrix}, \quad \begin{bmatrix} A & C \\ C & A \end{bmatrix},$$

a każda taka podmacierz zawiera wszystkie kolumny $\begin{bmatrix} i \\ j \end{bmatrix}$, $0 \leqslant i, j \leqslant 2m$, $i \neq j$. Zachęcamy czytelnika do uzupełnienia wszystkich szczegółów dowodu, gdyż dopiero wtedy można ocenić jak bardzo pomysłowa jest to konstrukcja. □

Otrzymujemy już teraz łatwo

TWIERDZENIE 9.7. *Dla dowolnego $n \equiv 10 \pmod{12}$ istnieje para ortogonalnych kwadratów łacińskich rzędu n.*

Dowód. Na mocy twierdzenia 9.5 dla dowolnego $k \geqslant 0$ istnieje para ortogonalnych kwadratów łacińskich rzędu $4k+3$. W myśl lematu 9.6 istnieje więc para ortogonalnych kwadratów łacińskich rzędu $3(4k+3)+1 = 12k+10$. □

Ze względu na twierdzenie 9.2 ortogonalne kwadraty łacińskie mogą być pomocne przy badaniu istnienia płaszczyzn rzutowych. Dla przykładu: Istnienie płaszczyzny rzutowej rzędu 10 jest równoważne istnieniu zbioru dziewięciu ortogonalnych kwadratów łacińskich rzędu 10. Tymczasem największy znany zbiór tego typu składa się z dwóch kwadratów. Jeśli rzeczywiście $N(10) = 2$, to wykazanie nieistnienia trzech ortogonalnych kwadratów łacińskich rzędu 10 może się okazać łatwiejsze niż wykazanie nieistnienia płaszczyzny rzutowej rzędu 10 — w pierwszym przypadku mamy do czynienia z macierzami wymiaru 10×10, w drugim zaś 111×111.

§ 10. Macierze Hadamarda

W 1893 roku francuski matematyk Jacques Hadamard udowodnił następujące twierdzenie:

Dla dowolnej macierzy zespolonej $X = [x_{ij}]$ wymiaru $n \times n$

$$|\det X|^2 \leqslant \prod_{i=1}^{n} \left(\sum_{j=1}^{n} |x_{ij}|^2 \right).$$

Jeśli każdy element macierzy X jest równy 1 lub -1, to nierówność ta przyjmuje postać $|\det X|^2 \leqslant n^n$ czyli,

$$|\det X| \leqslant n^{n/2};$$

co więcej, można wykazać, że równość zachodzi wtedy i tylko wtedy, gdy $XX^T = nI$. Taka jest historia definicji, którą teraz podamy: Macierz H wymiaru $n \times n$ o elementach $+1$, -1 nazywamy *macierzą Hadamarda rzędu n*, jeśli

$$HH^T = nI. \tag{10.1}$$

Choć macierze Hadamarda pojawiły się w związku z problemem dotyczącym wyznaczników, już sam Hadamard przeczuwał, że mogą one znaleźć wiele innych zastosowań. I nie mylił się. Dziś macierze Hadamarda używane są w teorii kodów, teorii informacji, układaniu rozgrywek brydżowych i wielu innych dziedzinach. Jako ciekawostkę można podać fakt, że w wyprawie sondy Mariner na Marsa w roku 1969 system telemetryczny używał kodu korygującego błędy opartego na pewnej macierzy Hadamarda rzędu 32. Doskonały przegląd zastosowań macierzy Hadamarda można znaleźć w monografii: Wallis, Street i Wallis [1] (p. rozdział

XI części trzeciej). Warto zauważyć, że w większości tych zastosowań wyznacznik macierzy Hadamarda jest zupełnie nieistotny.

Teoria macierzy Hadamarda jest dziś bogatym działem kombinatoryki mającym wiele ciekawych związków, między innymi z konfiguracjami, płaszczyznami rzutowymi i zbiorami różnicowymi. Niektóre z nich poznamy w tym paragrafie.

Zaczniemy od elementarnych wniosków z definicji. Równość (10.1) mówi, że każde dwa różne wiersze macierzy H są ortogonalne, tzn. ich iloczyn skalarny jest równy zeru. Również każde dwie różne kolumny są ortogonalne, gdyż z (10.1) otrzymujemy $H^T = nH^{-1}$, czyli

$$H^T H = nH^{-1} = nI.$$

Wniosek 10.1. *H jest macierzą Hadamarda wtedy i tylko wtedy, gdy H^T jest macierzą Hadamarda.*

Łatwo widać, że permutacja wierszy i kolumn, jak również pomnożenie dowolnego wiersza i kolumny przez -1, nie narusza ortogonalności. Dwie macierze Hadamarda będziemy nazywali *równoważnymi*, jeśli jedną można otrzymać z drugiej przez stosowanie tych operacji. Dla każdej macierzy Hadamarda H istnieje równoważna jej *znormalizowana macierz Hadamarda*, tzn. taka, której pierwszy wiersz i pierwsza kolumna zawiera wyłącznie elementy $+1$; wystarczy pomnożyć przez -1 te wiersze macierzy H, które zawierają -1 w pierwszej kolumnie, oraz te kolumny, które zawierają -1 w pierwszym wierszu.

Łatwo skonstruować macierze Hadamarda rzędu 1 i 2:

$$[1], \quad \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Załóżmy teraz, że H jest znormalizowaną macierzą Hadamarda rzędu $n \geqslant 3$. Po ewentualnej permutacji kolumn jej pierwsze trzy wiersze możemy przedstawić następująco:

$$\text{(10.2)} \qquad \left[\begin{array}{c:c:c:c} \overset{t}{} & \overset{x}{} & \overset{y}{} & \overset{z}{} \\ 1 \ldots 1 & 1 \ldots \ 1 & 1 \ldots \ 1 & 1 \ldots \ 1 \\ 1 \ldots 1 & 1 \ldots \ 1 & -1 \ldots -1 & -1 \ldots -1 \\ 1 \ldots 1 & -1 \ldots -1 & 1 \ldots \ 1 & -1 \ldots -1 \end{array}\right].$$

Biorąc pod uwagę fakt, że te trzy wiersze są parami ortogonalne otrzymujemy następujący układ równań

$$\begin{aligned} & t+x+y+z = n, \\ & t+x-y-z = 0 \quad \text{(wiersz 1)} \perp \text{(wiersz 2)}, \\ & t-x+y-z = 0 \quad \text{(wiersz 1)} \perp \text{(wiersz 3)}, \\ & t-x-y+z = 0 \quad \text{(wiersz 2)} \perp \text{(wiersz 3)}. \end{aligned}$$

Jego rozwiązaniem jest $t = x = y = z = n/4$. Mamy zatem następny wniosek:

Wniosek 10.2. *Jeśli istnieje macierz Hadamarda rzędu n, to* $n = 1, 2$ *lub* $n \equiv 0 \pmod 4$.

Przypuszcza się, że macierz Hadamarda rzędu n istnieje dla dowolnego $n \equiv 0 \pmod 4$. Pierwszym wątpliwym przypadkiem jest $n = 188$.

Każdej znormalizowanej macierzy Hadamarda H rzędu $4t$ odpowiada w naturalny sposób konfiguracja kwadratowa o parametrach

$$v = 4t-1, \quad k = 2t-1, \quad \lambda = t-1. \tag{10.3}$$

Istotnie, usuńmy z macierzy H pierwszy wiersz i pierwszą kolumnę oraz zamieńmy każdy element -1 na 0. Łatwo widać, że otrzymana w ten sposób macierz zero-jedynkowa wymiaru $(4k-1)\times(4k-1)$ ma $2t-1$ jedynek w każdym wierszu i każdej kolumnie, zaś iloczyn skalarny dwóch wierszy równy jest $t-1$ (por. (10.2)). Otrzymaliśmy więc macierz incydencji konfiguracji kwadratowej o parametrach (10.3). Konstrukcja ta jest odwracalna: jeśli A jest macierzą incydencji konfiguracji o parametrach (10.3), to

$$H = \left[\begin{array}{c|c} 1 & 1 \ldots 1 \\ \hline 1 & \\ \vdots & 2A-J \\ 1 & \end{array}\right]$$

jest znormalizowaną macierzą Hadamarda rzędu $4t$. Mamy więc

Twierdzenie 10.3. *Macierz Hadamarda rzędu 4t istnieje wtedy i tylko wtedy, gdy istnieje konfiguracja kwadratowa o parametrach* $v = 4t-1$, $k = 2t-1$, $\lambda = t-1$.

Konfiguracje o parametrach (10.3) oraz ich konfiguracje dopełnieniowe (p. § 2) o parametrach

$$\bar{v} = 4t-1, \quad \bar{k} = 2t, \quad \bar{\lambda} = t$$

nazywamy *konfiguracjami Hadamarda.*

Wykażemy teraz kilka metod konstrukcji macierzy Hadamarda. Przypomnijmy, że przez iloczyn Kroneckera macierzy $A = [a_{ij}]$ wymiaru $n \times m$ przez macierz B wymiaru $r \times s$ rozumiemy następującą macierz wymiaru $nr \times ms$:

$$A \times B = \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1m}B \\ a_{21}B & a_{22}B & \ldots & a_{2m}B \\ \vdots & \vdots & & \vdots \\ a_{n1}B & a_{n2}B & \ldots & a_{nm}B \end{bmatrix}.$$

Lemat 10.4. *Jeśli* H_1, H_2 *są macierzami Hadamarda rzędu odpowiednio* n_1, n_2, *to* $H = H_1 \times H_2$ *jest macierzą Hadamarda rzędu* $n = n_1 n_2$.

Dowód. Oczywiście każdy element macierzy H jest równy $+1$ lub -1. Mamy sprawdzić, że wiersze i-ty i j-ty są ortogonalne dla dowolnych i, j, $1 \leqslant i < j \leqslant n$. Jeśli $i \not\equiv j \pmod{n_2}$, to fakt ten wynika bezpośrednio z ortogonalności wierszy macierzy H_2, w przypadku zaś $i \equiv j \pmod{n_2}$, $i \neq j$, jest to wniosek z ortogonalności wierszy macierzy H_1 o numerach $\lceil i/n_2 \rceil$ i $\lceil j/n_2 \rceil$. □

W szczególności, każdą macierz Hadamarda możemy „podwoić" mnożąc przez nią $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. Dla przykładu

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \left[\begin{array}{cccc:cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ \hdashline 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right]$$

Skoro macierze Hadamarda równoważne są konfiguracjom kwadratowym, to możemy użyć do ich konstrukcji zbiory różnicowe o parametrach (10.3); zbiory takie nazwaliśmy w § 7 zbiorami różnicowymi Hadamarda. Przykładem takich zbiorów różnicowych są zbiory typu Q opisane w § 7.

Opiszemy teraz dwie konstrukcje pochodzące od R. E. A. C. Paley'a, z których pierwsza jest w istocie równoważna wykorzystaniu zbioru różnicowego typu Q. Niech $q = p^m$, gdzie p jest nieparzystą liczbą pierwszą i $m \geqslant 1$. Ustawmy elementy ciała $GF(q)$ w dowolny ciąg $a_0, \ldots, a_{q-1}$. Określmy macierz $Q = [q_{ij}]$ wymiaru $q \times q$ następująco:

$$q_{ij} = \chi(a_i - a_j),$$

gdzie χ jest charakterem kwadratowym w $GF(q)$ (p. Dodatek). Z własności charakteru kwadratowego wynika (por. Dodatek, twierdzenie 34), że

$$q_{ij} = \chi(-1)\chi(a_j - a_i) = \chi(-1)q_{ji}.$$

Lecz

$$\chi(-1) = \begin{cases} 1, & \text{jeśli } q \equiv 1 \pmod 4, \\ -1, & \text{jeśli } q \equiv 3 \pmod 4), \end{cases}$$

Q jest więc macierzą symetryczną ($Q^T = Q$) dla $q \equiv 1 \pmod 4$ i skośnie symetryczną ($Q^T = -Q$) dla $q \equiv 3 \pmod 4$. W obu przypadkach przekątna główna składa się z samych zer.

LEMAT 10.5. *$QQ^T = qI - J$, oraz suma elementów w dowolnym wierszu i dowolnej kolumnie macierzy Q jest równa zeru.*

Dowód. Niech $QQ^T = B = [b_{ij}]$. Zgodnie z twierdzeniem z Dodatku

$$b_{ij} = \sum_{k=0}^{q-1} q_{ik}q_{jk} = \sum_{k=0}^{q-1} \chi(a_i - a_k)\chi(a_j - a_k) =$$

$$= \sum_{a \in GF(q)} \chi(a)\chi(a + a_j - a_i) = \sum_{a \in GF(q)\setminus\{0\}} \chi(a)\chi\left(a \cdot \left(1 + \frac{a_j - a_i}{a}\right)\right) =$$

$$= \sum_{a \in GF(q)\setminus\{0\}} \chi\left(1 + \frac{a_j - a_i}{a}\right) = \begin{cases} q-1, & \text{jeśli } i = j, \\ -1, & \text{jeśli } i \neq j. \end{cases}$$

W przypadku $i \neq j$ korzystamy z tego, że $\sum_{a \in GF(q)} \chi(a) = 0$ oraz $1 + (a_j - a_i)/a$ przebiega wszystkie elementy ciała różne od jedności, gdy a przebiega wszystkie elementy niezerowe ciała. □

Pierwsza konstrukcja Paley'a: $q \equiv 3 \pmod 4$. Tworzymy macierz

$$S = \left[\begin{array}{c|c} 0 & 1\ 1 \dots 1 \\ \hline -1 & \\ -1 & \\ \vdots & Q \\ -1 & \end{array}\right].$$

Macierz Q jest skośnie symetryczna, a więc również

$$S^T = -S.$$

Z lematu 10.5 wynika, że

$$SS^T = qI.$$

Macierz

$$H = S + I$$

jest macierzą Hadamarda rzędu $q+1$, gdyż

$$HH^T = (S+I)(S^T+I) = SS^T + S + S^T + I = qI + I = (q+1)I.$$

Przyjmując na przykład $q = 7$ otrzymujemy następującą macierz Hadamai rzędu 8 ($-$ oznacza -1):

$$H = \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline - & 1 & - & - & 1 & - & 1 & 1 \\ - & 1 & 1 & - & - & 1 & - & 1 \\ - & 1 & 1 & 1 & - & - & 1 & - \\ - & - & 1 & 1 & 1 & - & - & 1 \\ - & 1 & - & 1 & 1 & 1 & - & - \\ - & - & 1 & - & 1 & 1 & 1 & - \\ - & - & - & 1 & - & 1 & 1 & 1 \end{array}\right].$$

Macierze otrzymane przez pierwszą konstrukcję Paley'a mają pewną szczególną postać, mianowicie

$$H = S+I, \quad \text{gdzie } S^T = -S.$$

Macierze Hadamarda tej postaci nazywamy *skośnymi*.

Otrzymaliśmy zatem następujące

TWIERDZENIE 10.6. *Jeśli q jest potęgą liczby pierwszej i* $q \equiv 3 \pmod 4$, *to istnieje skośna macierz Hadamarda rzędu* $q+1$.

Druga konstrukcja Paley'a: $q \equiv 1 \pmod 4$. Tworzymy macierz

$$S = \left[\begin{array}{c:ccc} 0 & 1 & 1 \ldots & 1 \\ \hdashline 1 & & & \\ 1 & & & \\ \vdots & & Q & \\ 1 & & & \end{array}\right]$$

Analogicznie jak poprzednio otrzymujemy równości

$$S^T = S,$$
$$SS^T = SS = qI.$$

Niech

$$H = \left[\begin{array}{c:c} S+I & S-I \\ \hdashline S-I & -S-I \end{array}\right].$$

Wykażemy teraz, że H jest macierzą Hadamarda rzędu $2q+2$

$$HH^T = \left[\begin{array}{c:c} (S+I)^2+(S-I)^2 & 0 \\ \hdashline 0 & (S-I)^2+(S+I)^2 \end{array}\right] =$$

$$= \left[\begin{array}{c:c} 2qI+2I & 0 \\ \hdashline 0 & 2qI+2I \end{array}\right] = (2q+2)I.$$

A oto macierz Hadamarda rzędu 12 otrzymana przez zastosowanie drugiej konstrukcji Paley'a:

$$\left[\begin{array}{cccccc:cccccc}
1 & 1 & 1 & 1 & 1 & 1 & - & 1 & 1 & 1 & 1 & 1 \\
1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - & 1 \\
1 & 1 & 1 & 1 & - & - & 1 & 1 & - & 1 & - & - \\
1 & - & 1 & 1 & 1 & - & 1 & - & 1 & - & 1 & - \\
1 & - & 1 & 1 & 1 & 1 & 1 & - & - & 1 & - & 1 \\
1 & 1 & - & - & 1 & 1 & 1 & 1 & - & - & 1 & - \\
\hdashline
- & 1 & 1 & 1 & 1 & 1 & - & - & - & - & - & - \\
1 & - & 1 & - & - & 1 & - & - & - & 1 & 1 & - \\
1 & 1 & - & 1 & - & - & - & - & - & - & 1 & 1 \\
1 & - & 1 & - & 1 & - & - & 1 & - & - & - & 1 \\
1 & - & - & 1 & - & 1 & - & 1 & 1 & - & - & - \\
1 & 1 & - & - & 1 & - & - & - & 1 & 1 & - & -
\end{array}\right].$$

Druga konstrukcja Hadamarda daje dla odmiany macierze symetryczne. Odnotujmy ten fakt:

TWIERDZENIE 10.7. *Jeśli q jest potęgą liczby pierwszej i $q \equiv 1 \pmod 4$, to istnieje symetryczna macierz Hadamarda rzędu $2q+2$.*

Inną ciekawą metodę konstrukcji macierzy Hadamarda podał J. Williamson [1]. Oparta jest ona na następującej macierzy wymiaru $4t \times 4t$:

$$W = \left[\begin{array}{c:c:c:c}
A & B & C & D \\
\hdashline
-B & A & -D & C \\
\hdashline
-C & D & A & -B \\
\hdashline
-D & -C & B & A
\end{array}\right], \tag{10.4}$$

gdzie A, B, C, D są pewnymi macierzami wymiaru $t \times t$.

Jeśli założymy, że macierze A, B, C, D parami komutują, to łatwo sprawdzić, że

$$WW^T = \left[\begin{array}{c:c:c:c}
M & 0 & 0 & 0 \\
\hdashline
0 & M & 0 & 0 \\
\hdashline
0 & 0 & M & 0 \\
\hdashline
0 & 0 & 0 & M
\end{array}\right].$$

gdzie $M = A^2+B^2+C^2+D^2$. Jeśli więc dobierzemy macierze A, B, C, D parami komutujące, o elementach $+1$, -1 i takie, że $A^2+B^2+C^2+D^2 = 4tI$, to (10.4) staje się macierzą Hadamarda. Nie będziemy się tu zagłębiali w metody doboru macierzy A, B, C, D, podamy jedynie przykład. Niech $t = 3$. Przyjmujemy

$$A = J = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \qquad B = C = D = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}.$$

Mamy wtedy

$$A^2+B^2+C^2+D^2 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix} + 3\begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} = 12I.$$

Przy takich macierzach A, B, C, D otrzymujemy z (10.4) macierz Hadamarda rzędu 12.

§ 11. Systemy trójek Steinera

Zajmiemy się obecnie pewnym bardzo szczególnym przypadkiem konfiguracji kombinatorycznych, mianowicie konfiguracjami o parametrach $k = 3$, $\lambda = 1$. Tradycyjnie są one zwane *systemami trójek Steinera*. Parametr v takiej konfiguracji spełnia, jak wiemy, zależności

$$v-1 \equiv 0 \pmod 2, \qquad v(v-1) \equiv 0 \pmod 6$$

(p. twierdzenie 1.4), czyli

(11.1) $$v = 1, 3 \pmod 6.$$

Problem, czy warunek ten jest wystarczający dla istnienia systemu trójek Steinera, został postawiony w 1853 roku przez Steinera [1] i rozwiązany pozytywnie przez Reissa [1] w 1859 roku. Stosunkowo niedawno okazało się jednak, że zagadnienie to było już w 1847 r. sformułowane i rozwiązane przez Thomasa Kirkmana [1]. Przytoczymy tu jego rozwiązanie.

Parametr v będziemy nazywali *rzędem* systemu trójek Steinera. Nie wykluczamy z rozważań przypadków $v = 1$ i $v = 3$ odpowiadających konfiguracjom zdegenerowanym. Przez *niepełny system trójek rzędu* v na zbiorze $X = \{x_0, x_1, \ldots, x_v\}$ będziemy rozumieli dowolną rodzinę podzbiorów trójelementowych zbioru X taką, że — po ewentualnym przenumerowaniu elementów zbioru X — każda para $\{x_i, x_j\}$, $0 \leqslant i < j \leqslant v$, zawarta jest w dokładnie jednym podzbiorze, z wyjątkiem par

(11.2) $$\{x_i, x_{(i+1)\bmod v}\}, \qquad 0 \leqslant i < v,$$

które nie występują w żadnych podzbiorach. Zauważmy, że pary (11.2) tworzą cykl długości v omijający element x_v.

Każda trójka zawiera 3 pary, wszystkich zaś par jest $\binom{v}{2} = \frac{1}{2}v(v-1)$. A zatem system trójek Steinera rzędu v składa się z

(11.3) $$b = \frac{v(v-1)}{6}$$

trójek. Jest oczywiste, że jeśli pewna rodzina $\frac{1}{6}v(v-1)$ podzbiorów trójelementowych zbioru v-elementowego ma tę własność, że każda para zawarta jest w co najmniej jednym podzbiorze, to każda para pojawia się w dokładnie jednym podzbiorze, i w konsekwencji rodzina ta jest systemem trójek Steinera rzędu v.

W niepełnym systemie trójek rzędu v występuje w sumie $\binom{v+1}{2} - v = \frac{1}{2}v(v-1)$ par — tyle samo, co w systemie trójek Steinera rzędu v. Ilość trójek musi więc też być równa $\frac{1}{6}v(v-1)$. Spośród nich $\frac{1}{2}v$ zawiera x_v. Otrzymane w ten sposób warunki $v \equiv 0 \pmod 2$, $v(v-1) \equiv 0 \pmod 6$ możemy połączyć w następujący warunek konieczny istnienia niepełnego systemu trójek rzędu v:

(11.4) $$v \equiv 0, 4 \pmod 6.$$

LEMAT 11.1. *Jeśli istnieje system trójek Steinera rzędu v, to istnieje system trójek Steinera rzędu $2v+1$ oraz niepełny system trójek rzędu $2v-2$.*

Dowód. Niech S będzie systemem trójek Steinera rzędu v na zbiorze $\{x_1, \ldots, x_v\}$. Zdefiniujemy najpierw pewien system trójek Steinera S^* rzędu $2v+1$ na zbiorze $\{x_1, \ldots, x_v, y_1, \ldots, y_v, z\}$. Będzie się on składał z następujących trójek:

(i) trójki systemu S,

(ii) $\{x_i, y_j, y_k\}$ dla $i \equiv j+k \pmod v$, $j < k$, $1 \leqslant i, j, k \leqslant v$,

(iii) $\{x_i, y_j, z\}$ dla $i \equiv 2j \pmod v$, $1 \leqslant i, j \leqslant v$.

Sprawdzimy teraz, że jest to istotnie system trójek Steinera rzędu $2v+1$. Wszystkie pary postaci $\{x_i, x_j\}$, $i \neq j$, występują oczywiście w trójkach typu (i). Zgodnie z (11.1) v jest nieparzyste. W konsekwencji dla dowolnego i istnieje j takie, że $i \equiv 2j \pmod v$, $1 \leqslant i, j \leqslant v$. Oznacza to, że każda para zawierająca z pojawia się w pewnej trójce typu (iii). Jest jasne, że każda para $\{y_j, y_k\}$, $j < k$, jest zawarta w pewnej trójce typu (ii). Pozostają pary postaci $\{x_i, y_j\}$. Lecz dla dowolnych i, j istnieje $k \geqslant j$ takie, że $i \equiv k+j \pmod v$. Para $\{x_i, y_j\}$ jest więc zawarta w pewnej trójce typu (iii), jeśli $k = j$, oraz typu (ii), jeśli $k > j$. Wszystkich trójek jest $\frac{1}{6}v(v-1)+\frac{1}{2}v(v-1)+v = \frac{1}{6}(2v+1)[(2v+1)-1]$, a więc S^* jest systemem trójek Steinera rzędu $2v+1$.

Z systemu S^* otrzymujemy niepełny system trójek N^* rzędu $2v-2$ przez usunięcie elementów y_1, y_v oraz wszystkich trójek zawierających co najmniej jeden z nich:

Typ trójek	Usuniete trójki	Występujące w nich pary nie zawierające y_1, y_v
(ii)	$\{x_i, y_i, y_v\}$, $1 \leqslant i \leqslant v-1$	$\{x_i, y_i\}$, $2 \leqslant i \leqslant v-1$
(ii)	$\{x_i, y_{i-1}, y_1\}$, $3 \leqslant i \leqslant v$	$\{x_i, y_{i-1}\}$, $3 \leqslant i \leqslant v$
(iii)	$\{x_2, y_1, z\}$	$\{x_2, z\}$
(iii)	$\{x_v, y_v, z\}$	$\{x_v, z\}$

Wystarczy teraz zauważyć, że usunięte pary tworzą następujący cykl długości $2v-2$ omijający x_1:

$$\{z, x_2\}, \{x_2, y_2\}, \{y_2, x_3\}, \{x_3, y_3\}, \ldots, \{x_{v-1}, y_{v-1}\}, \{y_{v-1}, x_v\}, \{x_v, z\}. \quad \square$$

Zilustrujemy opisaną konstrukcję na przykładzie $v = 3$. System trójek Steinera rzędu 3 składa się z jednej trójki $\{x_1, x_2, x_3\}$. Otrzymujemy z niego następujący system trójek Steinera rzędu 7:

$$(11.5) \qquad \begin{array}{c} \\ x_1 \\ x_2 \\ x_3 \\ y_1 \\ y_2 \\ y_3 \\ z \end{array} \left[\begin{array}{c:ccc:ccc} \text{(i)} & & \text{(ii)} & & & \text{(iii)} & \\ 1 & & 1 & & & 1 & \\ 1 & & & 1 & 1 & & \\ 1 & 1 & & & & & 1 \\ \hdashline & 1 & 1 & & 1 & & \\ & 1 & & 1 & & 1 & \\ & & 1 & 1 & & & 1 \\ \hdashline & & & & 1 & 1 & 1 \end{array}\right].$$

Po usunięciu elementów y_1, y_3 oraz trójek zawierających co najmniej jeden z nich otrzymujemy następujący niepełny system trójek rzędu 4:

$$\begin{array}{c} x_1 \\ x_2 \\ x_3 \\ y_2 \\ z \end{array} \left[\begin{array}{cc} 1 & 1 \\ 1 & \\ 1 & \\ & 1 \\ & 1 \end{array}\right] \begin{array}{cccc} \multicolumn{4}{c}{\text{brakujące pary}} \\ & & & \\ * & * & & \\ & & * & * \\ & * & * & \\ * & & & * \end{array} \qquad \begin{array}{c} z \\ x_2 \\ y_2 \\ x_3 \\ x_1 \end{array} \left[\begin{array}{cc} & 1 \\ 1 & \\ & 1 \\ 1 & \\ 1 & 1 \end{array}\right] \begin{array}{cccc} \multicolumn{4}{c}{\text{brakujące pary}} \\ * & & & * \\ * & * & & \\ & * & * & \\ & & * & * \\ & & & \end{array}$$

LEMAT 11.2. *Jeśli istnieje niepełny system trójek rzędu $v > 0$, to istnieje system trójek Steinera rzędu $2v+1$ oraz niepełny system trójek rzędu $2v-2$.*

D o w ó d. Niech N będzie niepełnym systemem trójek rzędu v na zbiorze $\{x_0, x_1, \ldots, x_v\}$. Wobec warunku (11.4) możemy napisać $v = 2u$. Określamy trójki systemu Steinera rzędu $2v+1$ na zbiorze $\{x_0, x_1, \ldots, x_v, y_1, \ldots, y_v\}$ następująco:

(i) trójki systemu K,

(ii) $\{x_i, x_{(i+1) \bmod v}, y_{i+1}\}$ dla $0 \leqslant i < v$,

(iii) $\{x_i, y_j, y_k\}$ dla $j+k \equiv 2i+1 \pmod{v-1}$, $1 \leqslant j < k-1 \leqslant v-2$, $1 \leqslant i \leqslant v-2$,
(iv) $\{x_i, y_j, y_v\}$ dla $2j \equiv 2i+1 \pmod{v-1}$, $1 \leqslant j \leqslant v-1$, $1 \leqslant i \leqslant v-2$,
(v) $\{x_0, y_{2j}, y_{2j+1}\}$, $\{x_{v-1}, y_{2j-1}, y_{2j}\}$ dla $1 \leqslant j < u$,
(vi) $\{x_v, y_j, y_{v-j}\}$ dla $1 \leqslant j < u$,
(vii) $\{x_v, y_u, y_v\}$.

Sprawdzimy teraz, że jest to rzeczywiście system trójek Steinera rzędu $2v+1$. Wykażemy najpierw, że w trójkach (i)–(vii) występują wszystkie możliwe pary. Dowód tego faktu rozbijemy na trzy przypadki:

I. Pary $\{x_i, x_j\}$, $0 \leqslant i < j \leqslant v$. Występują one oczywiście w trójkach postaci (i), (ii).

II. Pary $\{y_j, y_k\}$, $1 \leqslant j < k \leqslant v$. Rozpatrzmy najpierw przypadek $k = v$. Zauważmy, że jeśli $2j \neq v$, to istnieje dokładnie jedno i, $1 \leqslant i \leqslant v-2$ takie, że $2j+(v-1) = 2i+1$ lub $2j-(v-1) = 2i+1$. A zatem wszystkie pary $\{y_j, y_v\}$, $j \neq u$, pojawiają się w trójkach typu (iv). Para $\{y_u, y_v\}$ występuje w trójce (vii). W dalszym ciągu będziemy zakładali, że $k \leqslant v-1$. Dla $j+1 = k$ wszystkie pary $\{y_j, y_k\}$ występują w trójkach typu (v). Niech zatem $|j-k| \geqslant 2$. Podobnie jak poprzednio, jeśli $j+k \neq v$, to istnieje dokładnie jedno i, $1 \leqslant i \leqslant v-2$ takie, że $j+k \equiv 2i+1 \pmod{v-1}$, co oznacza, iż $\{y_j, y_k\}$ pojawia się w trójce typu (iv). Z kolei przypadek $j+k = v$ odpowiada trójkom typu (vi).

III. Pary $\{x_i, y_j\}$, $0 \leqslant i \leqslant v$, $1 \leqslant j \leqslant v$. Rozpatrzmy najpierw przypadek $i = 0$. Zauważmy, że pary $\{x_0, y_1\}$, $\{x_0, y_v\}$ występują w trójkach typu (ii), natomiast pary $\{x_0, y_j\}$, $2 \leqslant j \leqslant v-1$ w trójkach typu (v). Niech teraz $i = v$. Pary $\{x_v, y_u\}$, $\{x_v, y_v\}$ występują w trójce (vii), zaś pary $\{x_v, y_j\}$, $j \neq u$, $j \neq v$ w trójkach typu (vi). Rozpatrzmy jeszcze szczególny przypadek $i = v-1$. Pary $\{x_{v-1}, y_{v-1}\}$, $\{x_{v-1}, y_v\}$ są zawarte w trójkach typu (ii), a wszystkie pary $\{x_{v-1}, y_j\}$, $1 \leqslant j \leqslant v-2$, pojawiają się w trójkach typu (v). W dalszym ciągu zakładamy, że $1 \leqslant i \leqslant v-2$.

Zauważmy, że dla dowolnych i, j istnieje dokładnie jedno k takie, że $1 \leqslant k \leqslant v-1$ oraz $j+k \equiv 2i+1 \pmod{v-1}$. Mogą zachodzić następujące trzy przypadki: $k = j$, $|k-j| = 1$, $|k-j| \geqslant 2$. Jeśli $k = j$, to para $\{x_i, y_j\}$ występuje w trójce typu (iv). Jeśli $|k-j| = 1$, to musi być $j+k = 2j+1 = 2i+1$, czyli $i = j$, lub też $j+k = 2(j-1)+1 = 2i+1$, czyli $j = i+1$. W obu przypadkach para $\{x_i, y_j\}$ pojawia się w pewnej trójce typu (ii). Jeśli wreszcie $|k-j| \geqslant 2$, to para $\{x_i, x_j\}$ jest oczywiście zawarta w pewnej trójce typu (iii).

Łatwo sprawdzić, że liczba trójek poszczególnych typów jest następująca:

(i) $\frac{1}{6}v(v-1)$, (iv) $v-2$,
(ii) v, (v) $v-2$,
(iii) $\binom{v-1}{2}-(v-2)-(\frac{1}{2}v-1) =$ (vi) $\frac{1}{2}v-1$,
$= \frac{1}{2}v^2-3v+4$, (vii) 1.

Daje to, po zsumowaniu, $\frac{1}{6}(2v+1)[(2v+1)-1]$ trójek. Otrzymaliśmy więc system trójek Steinera rzędu $2v+1$.

Wykażemy teraz, że usuwając elementy y_1, y_{v-1} oraz wszystkie trójki zawierające co najmniej jeden z nich otrzymujemy pewien niepełny system trójek N^* rzędu $2v-2$.

Typ trójek	Usunięte trójki	Występujące w nich pary nie zawierające y_1, y_{v-1}	Typ par
(ii)	$\{x_0, x_1, y_1\}$	$\{x_0, x_1\}$	(1)
(ii)	$\{x_{v-2}, x_{v-1}, y_{v-1}\}$	$\{x_{v-2}, x_{v-1}\}$	(2)
(iii)	$\{x_i, y_1, y_{2i}\}$, $2 \leqslant i \leqslant u-1$	$\{x_i, y_{2i}\}$, $2 \leqslant i \leqslant u-1$	(3)
(iii)	$\{x_i, y_1, y_{2i-v+1}\}$, $u+1 \leqslant i \leqslant v-2$	$\{x_{u+i}, y_{2i+1}\}$, $1 \leqslant i \leqslant u-2$	(4)
(iii)	$\{x_i, y_{2i+1}, y_{v-1}\}$, $1 \leqslant i \leqslant u-2$	$\{x_i, y_{2i+1}\}$, $1 \leqslant i \leqslant u-2$	(5)
(iii)	$\{x_i, y_{2i-v+2}, y_{v-1}\}$, $u \leqslant i \leqslant v-3$	$\{x_{u+i}, y_{2i+2}\}$, $0 \leqslant i \leqslant u-3$	(6)
(iv)	$\{x_u, y_1, y_v\}$	$\{x_u, y_v\}$	(7)
(iv)	$\{x_{u-1}, y_{v-1}, y_v\}$	$\{x_{u-1}, y_v\}$	(8)
(v)	$\{x_0, y_{v-2}, y_{v-1}\}$	$\{x_0, y_{v-2}\}$	(9)
(v)	$\{x_{v-1}, y_1, y_2\}$	$\{x_{v-1}, y_2\}$	(10)

Wystarczy teraz zauważyć, że brakujące pary tworzą dla $v \geqslant 6$ następujący cykl długości $2v-2$ omijający x_v:

$$\left.\begin{array}{cccc}
 & \overset{(1)}{\{x_0, x_1\}}, & \overset{(5)}{\{x_1, y_3\}}, & \overset{(4)}{\{y_3, x_{u+1}\}}, \\
\overset{(6)}{\{x_{u+1}, y_4\}}, & \overset{(3)}{\{y_4, x_2\}}, & \overset{(5)}{\{x_2, y_5\}}, & \overset{(4)}{\{y_5, x_{u+2}\}}, \\
\{x_{u+2}, y_6\}, & \{y_6, x_3\}, & \{x_3, y_7\}, & \{y_7, x_{u+3}\}, \\
\dots & \dots & \dots & \dots \\
\{x_{v-3}, y_{v-4}\}, & \{y_{v-4}, x_{u-2}\}, & \{x_{u-2}, y_{v-3}\}, & \{y_{v-3}, x_{v-2}\},
\end{array}\right\} 4(u-3) \text{ par}$$

$$\overset{(2)}{\{x_{v-2}, x_{v-1}\}}, \overset{(10)}{\{x_{v-1}, y_2\}}, \overset{(6)}{\{y_2, x_u\}}, \overset{(7)}{\{x_u, y_v\}}, \overset{(8)}{\{y_v, x_{u-1}\}}, \overset{(3)}{\{x_{u-1}, y_{v-2}\}}, \overset{(9)}{\{y_{v-2}, x_0\}}.$$

Dla $v < 6$ (tzn. $v = 4$) cykl ten wygląda nieco inaczej (p. poniższy przykład). □

Zastosujmy konstrukcję z lematu 11.2 do niepełnego systemu trójek rzędu 4, składającego się z trójek $\{x_1, x_3, x_4\}$, $\{x_0, x_2, x_4\}$:

$$(11.6) \qquad \begin{array}{c} \\ x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ \\ y_1 \\ y_2 \\ y_3 \\ y_4 \end{array}
\begin{array}{cc|cccc|cc|cc|c|c}
\multicolumn{2}{c}{(i)} & \multicolumn{4}{c}{(ii)} & \multicolumn{2}{c}{(iv)} & \multicolumn{2}{c}{(v)} & (vi) & (vii) \\
 & 1 & 1 & & & 1 & & & 1 & & & \\
1 & & 1 & 1 & & & & 1 & & & & \\
 & 1 & & 1 & 1 & & 1 & & & & & \\
1 & & & & 1 & 1 & & & & 1 & & \\
1 & 1 & & & & & & & & & 1 & 1 \\
\hline
 & & 1 & & & & 1 & & & 1 & 1 & \\
 & & & 1 & & & & & 1 & 1 & & 1 \\
 & & & & 1 & & & 1 & 1 & & 1 & \\
 & & & & & 1 & 1 & 1 & & & & 1
\end{array}$$

Ze skonstruowanego w ten sposób systemu trójek Steinera rzędu 9 otrzymujemy niepełny system trójek rzędu 6 przez usunięcie elementów y_1, y_3 oraz wszystkich trójek zawierających co najmniej jeden z nich:

						Brakujące pary					
x_0	1			1		*				*	
x_1		1	1			*			*		
x_2	1		1				*	*			
x_3		1		1			*				*
x_4	1	1			1						
y_2			1		1					*	*
y_4				1	1			*	*		

czyli

						Brakujące pary					
x_0	1			1		*					*
x_1		1	1			*	*				
y_4				1	1		*	*			
x_2	1		1					*	*		
x_3		1		1					*	*	
y_2			1		1					*	*
x_4	1	1			1						

Z lematów 11.1 i 11.2 otrzymujemy już łatwo twierdzenie o istnieniu systemów trójek Steinera. Przy okazji okaże się, że warunek (11.4) jest wystarczający dla istnienia niepełnego systemu trójek rzędu v.

TWIERDZENIE 11.3. *Dla dowolnego* $v \equiv 1, 3 \pmod 6$ *istnieje system trójek Steinera rzędu* v, *dla dowolnego zaś* $v \equiv 0, 4 \pmod 6$ *istnieje niepełny system trójek rzędu* v.

Dowód. Umówmy się, że przez system trójek rzędu v będziemy rozumieli system trójek Steinera rzędu v lub niepełny system trójek rzędu v. Wobec wzorów (11.1), (11.4) wystarczy wykazać, że dla dowolnego $v \geqslant 0$ nie będącego postaci $3k+2$ istnieje system trójek rzędu v. Stosujemy indukcję względem v. Dla $v = 0, 1$ jest to oczywiście prawdą. Załóżmy teraz, że $n > 2$ i n nie jest postaci $3k+2$, oraz że twierdzenie jest prawdziwe dla dowolnego $v < n$. Przyjmijmy $v = \frac{1}{2}(n-1)$, jeśli n jest nieparzyste, oraz $v = \frac{1}{2}(n+2)$, jeśli n jest parzyste. Mamy $n = 2v+1$ w pierwszym przypadku oraz $n = 2v-2$ w drugim. W obu przypadkach $v < n$, co więcej, z równości $2(3k+2)+1 = 3(2k+1)+2$, $2(3k+2)-2 = 6k+2$ wynika, że v nie jest postaci $3k+2$. Na mocy założenia indukcyjnego oraz lematów 11.1, 11.2 istnieje więc system trójek rzędu n. □

Warto tu wspomnieć o jeszcze jednym słynnym problemie pochodzącym od Kirkmana. Zazwyczaj znany on jest w następującym sformułowaniu: Nauczycielka prowadzi codziennie na spacer 15 uczennic ustawionych w trójki. Należy znaleźć takie ustawienia na siedem kolejnych dni, aby żadne dwie uczennice nie spotkały się więcej niż jeden raz w tej samej trójce. Problem ten jest oczywiście równoważny znalezieniu systemu trójek Steinera rzędu 15, którego 35 trójek można podzielić na 7 grup tak, by każda grupa stanowiła podział zbioru elementów systemu. Rozwiązaniem jest następujący system trójek:

poniedziałek	$\{1, 2, 9\}$,	$\{3, 4, 6\}$,	$\{7, 10, 15\}$,	$\{5, 11, 14\}$,	$\{8, 12, 13\}$,
wtorek	$\{1, 3, 10\}$,	$\{4, 5, 7\}$,	$\{8, 11, 9\}$,	$\{6, 12, 15\}$,	$\{2, 13, 14\}$,
środa	$\{1, 4, 11\}$,	$\{5, 6, 8\}$,	$\{2, 12, 10\}$,	$\{7, 13, 9\}$,	$\{3, 14, 15\}$,
czwartek	$\{1, 5, 12\}$,	$\{6, 7, 2\}$,	$\{3, 13, 11\}$,	$\{8, 14, 10\}$,	$\{4, 15, 9\}$,
piątek	$\{1, 6, 13\}$,	$\{7, 8, 3\}$,	$\{4, 14, 12\}$,	$\{2, 15, 11\}$,	$\{5, 9, 10\}$,
sobota	$\{1, 7, 14\}$,	$\{8, 2, 4\}$,	$\{5, 15, 13\}$,	$\{3, 9, 12\}$,	$\{6, 10, 11\}$,
niedziela	$\{1, 8, 15\}$,	$\{2, 3, 5\}$,	$\{6, 9, 14\}$,	$\{4, 10, 13\}$,	$\{7, 11, 12\}$.

Powyższy system trójek jest prostym przykładem *konfiguracji rozwiązywalnej*, tzn. takiej konfiguracji $\langle X, \mathscr{B}\rangle$, której zbiór bloków możemy przedstawić w postaci $\mathscr{B} = \mathscr{B}_1 \dot{\cup} \ldots \dot{\cup} \mathscr{B}_s$, gdzie $\mathscr{B}_i$, $1 \leqslant i \leqslant s$ są podziałami zbioru X. W konfiguracji rozwiązywalnej mamy oczywiście

$$v \equiv 0 \pmod{k},$$

lecz nie jest znany żaden ogólny warunek konieczny i dostateczny istnienia takich konfiguracji. Wiadomo jednak, że rozwiązywalny system trójek Steinera — zwany też *systemem trójek Kirkmana* — istnieje dla dowolnego $v \equiv 3 \pmod 6$ (p. Ray-Chaudhuri i Wilson [1]). Warto przy okazji wspomnieć, że dla $v \equiv 1 \pmod 6$ system trójek Steinera rzędu v można zawsze otrzymać z pewnej rodziny różnicowej o parametrach v, $k = 3$, $\lambda = 1$, $t = \frac{1}{6}(v-1)$ w grupie $\boldsymbol{Z}_v$ (p. Peltesohn [1]). Innymi słowy, dla $v \equiv 1 \pmod 6$ istnieje zawsze taki system trójek Steinera rzędu v, w którym pewne cykliczne przesunięcie punktów określa automorfizm systemu.

§ 12. Kwadraty Rooma

Wprowadził je do literatury kombinatorycznej w 1955 r. T. G. Room [1]. Okazało się jednak, że już około 1897 roku E. C. Howell zastosował obiekty równoważne — zwane dziś *rotacjami Howella* — do układania podwójnych rozgrywek brydżowych.

Kwadratem Rooma o boku n nazywamy tablicę R wymiaru $n \times n$, której każda klatka może być pusta lub zawierać nieuporządkowaną parę elementów zbioru $N = \{0, 1, \ldots, n\}$, jeśli spełnione są następujące warunki:

R1. *Każda nieuporządkowana para elementów zbioru N występuje w R dokładnie raz.*

R2. *Każdy element zbioru N pojawia się dokładnie raz w każdym wierszu i w każdej kolumnie.*

Jest jasne, że natura elementów zbioru N jest zupełnie nieistotna. Będziemy czasem przyjmowali jako N zbiór $(n+1)$-elementowy różny od $\{0, 1, \ldots, n\}$. Klatkę na przecięciu i-tego wiersza i j-tej kolumny będziemy nazywali klatką $\langle i, j\rangle$.

Związek z podwójnymi rozgrywkami brydżowymi jest następujący. Załóżmy, że w turnieju startuje $n+1$ par, które oznaczali będziemy liczbami $0, 1, \ldots, n$. Aby zapewnić wszystkim parom możliwie równe szanse, porównuje się wyniki uzyskane przez różne pary rozgrywające te same rozdania. Rozdań tych jest n i odpowiadają one kolumnom kwadratu Rooma, wiersze natomiast odpowiadają rundom turnieju. Jeśli w i-tej rundzie pary p i q rozgrywają przeciwko sobie j-te rozdanie, to klatka $\langle i, j\rangle$ kwadratu Rooma zawiera parę $\{p, q\}$, jeśli zaś j-te rozdanie nie jest w i-tej rundzie używane, to klatka ta jest pusta. Warunek R1 oznacza, że każde dwie pary (zawodników) grają przeciwko sobie dokładnie raz, warunek zaś R2 mówi, że każda para gra w każdej rundzie dokładnie raz oraz rozgrywa w ciągu turnieju każde rozdanie dokładnie raz.

W rzeczywistości kwadrat Rooma nie określa całkowicie rozgrywek, gdyż nie mówi, na której linii (NS czy EW) ma grać każda z par w każdym spotkaniu. Do problemu tego jeszcze powrócimy.

Zauważmy, że z faktu, iż każdy wiersz kwadratu Rooma zawiera $n+1$ elementów, które występują parami, wynika, że $n+1$ jest parzyste. A więc n musi być nieparzyste. Jest również oczywiste, że permutacja wierszy, kolumn, przenumerowanie elementów $0, 1, \ldots, n$, jak również transponowanie kwadratu Rooma nie narusza warunków R1, R2. Jeśli jeden kwadrat Rooma można otrzymać z drugiego używając tych operacji, to kwadraty te nazywamy *równoważnymi*.

Zajmiemy się teraz konstrukcją kwadratów Rooma. Istnieje oczywiście dokładnie jeden kwadrat Rooma o boku 1:

01

(parę $\{p, q\}$ będziemy oznaczali czasem przez pq). Jeśli istnieje kwadrat Rooma o boku 3, to możemy bez zmniejszenia ogólności przyjąć, że klatka $\langle 1, 1\rangle$ zawiera $\{0, 1\}$. Każdy wiersz i każda kolumna ma zawierać elementy $0, 1, 2, 3$, a więc para $\{2, 3\}$ musi występować zarówno w pierwszym wierszu jak i w pierwszej kolumnie, wbrew warunkowi R1. A zatem kwadrat Rooma o boku 3 nie istnieje.

W podobny sposób można wykazać, że nie istnieje kwadrat Rooma o boku 5 (p. zad. 63). Okazuje się, że dla wszystkich pozostałych (nieparzystych) wartości n kwadrat Rooma istnieje. Fakt ten nie jest bynajmniej oczywisty i do jego udowodnienia doprowadziły wspólne wysiłki wielu matematyków, wspomagane w dużym stopniu użyciem maszyn cyfrowych. Najdłużej opierała się tym wysiłkom wartość $n = 257$ — kwadrat Rooma o takim boku został skonstruowany przez australijskiego kombinatoryka W. D. Wallisa dopiero w 1972 r. (por. Wallis [1]).

Opiszemy teraz pewną metodę konstrukcji kwadratów Rooma pochodzącą od Stantona i Mullina [1].

Niech $n = 2s+1$ i niech G będzie dowolną grupą przemienną rzędu n. Przez *starter* w G będziemy rozumieli dowolny ciąg

$$S = \langle\{x_1, y_1\}, \ldots, \{x_s, y_s\}\rangle$$

nieuporządkowanych par elementów grupy G taki, że

(12.1) $$\{x_1, \ldots, x_s\} \cup \{y_1, \ldots, y_s\} = G \setminus \{0\},$$

(12.2) $$\{x_1 - y_1, \ldots, x_s - y_s\} \cup \{y_1 - x_1, \ldots, y_s - x_s\} = G \setminus \{0\}.$$

Sumatorem dla startera S nazywamy dowolny ciąg

$$A = \langle a_1, \ldots, a_s \rangle$$

parami różnych elementów niezerowych grupy G taki, że

(12.3) $$\{x_1 + a_1, \ldots, x_s + a_s\} \cup \{y_1 + a_1, \ldots, y_s + a_s\} = G \setminus \{0\}.$$

Oczywiście, wszystkie sumy $x_i + a_i$, $y_i + a_i$ są różne, podobnie jak różne są wszystkie różnice $x_i - y_i$, $y_i - x_i$ w (12.2).

Przykładem startera w grupie reszt modulo 7 jest

(12.4) $$S = \langle \{1, 6\}, \{2, 5\}, \{3, 4\} \rangle.$$

mamy bowiem następujące kongruencje modulo 7:

$$1 - 6 \equiv 2, \quad 2 - 5 \equiv 4, \quad 3 - 4 \equiv 6,$$
$$6 - 1 \equiv 5, \quad 5 - 2 \equiv 3, \quad 4 - 3 \equiv 1.$$

Ciąg

(12.5) $$A = \langle 2, 4, 1 \rangle$$

jest sumatorem dla S, gdyż

$$1 + 2 \equiv 3, \quad 2 + 4 \equiv 6, \quad 3 + 1 \equiv 4,$$
$$6 + 2 \equiv 1, \quad 5 + 4 \equiv 2, \quad 4 + 1 \equiv 5.$$

TWIERDZENIE 12.1. *Jeśli istnieje starter oraz sumator dla niego w pewnej grupie przemiennej rzędu nieparzystego n, to istnieje kwadrat Rooma o boku n.*

Dowód. Niech $S = \langle \{x_1, y_1\}, \ldots, \{x_s, y_s\} \rangle$ będzie starterem, $A = \langle a_1, \ldots, a_s \rangle$ zaś sumatorem dla niego w grupie przemiennej G rzędu $n = 2s+1$ o elementach $g_0 = 0, g_1, \ldots, g_{n-1}$. Skonstruujemy kwadrat Rooma, którego wiersze i kolumny odpowiadają elementom grupy G. Jego niepuste klatki będą zawierały pary nieuporządkowane elementów zbioru $\{\infty, g_0, \ldots, g_{n-1}\}$, gdzie $\infty \notin G$ jest pewnym dodatkowym elementem. Dla $0 \leqslant i, j \leqslant n-1$ klatka $\langle g_i, g_j \rangle$, tzn. klatka na przecięciu wiersza odpowiadającego g_i oraz kolumny odpowiadającej g_j,

zawiera $\{\infty, g_i\}$,	jeśli $i = j$,
zawiera $\{x_k + g_i, y_k + g_i\}$,	jeśli $g_i - g_j = a_k$,
jest pusta,	jeśli $g_i - g_j$ nie występuje w A, $i \neq j$.

Wykażemy teraz, że tak określona tablica jest kwadratem Rooma. Sprawdzimy najpierw warunek R1. Pary postaci $\{\infty, g_i\}$, $0 \leqslant i \leqslant n-1$, występują na przekątnej,

każda dokładnie raz. Jeśli $\{g, h\}$ jest dowolną parą nieuporządkowaną elementów grupy G, to na mocy (12.2) nasz starter zawiera parę $\{x_i, y_i\}$ taką, że

$$x_i - y_i = g - h \quad \text{lub} \quad y_i - x_i = g - h.$$

Określimy $b = h - y_i$ w pierwszym przypadku, i $b = g - y_i$ w drugim. Mamy wówczas

$$\{g, h\} = \{x_i + b,\ y_i + b\},$$

co oznacza, iż $\{g, h\}$ występuje w naszej tablicy (w wierszu odpowiadającym elementowi b i kolumnie odpowiadającej elementowi $b - a_i$). W każdym wierszu jest dokładnie $s+1$ niepustych klatek, zawierających $\{\infty, g_i\}$ oraz $\{x_k + g_i, y_k + y_i\}$, $1 \leqslant i \leqslant s$. W sumie daje to $n(s+1) = \frac{1}{2}n(n+1)$ niepustych klatek, tyle ile jest wszystkich par nieuporządkowanych elementów zbioru $\{\infty, g_0, \ldots, g_{n-1}\}$. Każda taka para występuje więc dokładnie raz.

Zauważmy, że wiersz odpowiadający g_i zawiera elementy

$$\infty,\ g_i,\ x_1 + g_i, \ldots, x_s + g_i,\ y_1 + g_i, \ldots, y_s + g_i.$$

Lecz z warunku (12.1) wynika, że są to elementy $\infty, g_0, \ldots, g_{n-1}$, w pewnej kolejności. Podobnie kolumna odpowiadająca g_j zawiera elementy

$$\infty,\ g_j \quad \text{oraz} \quad x_k + g_i,\ y_k + g_i \quad \text{dla } g_i - g_j = a_k,$$

czyli

$$\infty,\ g_j \quad \text{oraz} \quad x_k + a_k + g_j,\ y_k + a_k + g_j \quad \text{dla } 1 \leqslant k \leqslant s.$$

Z warunku (12.3) wynika, że są to dokładnie elementy $\infty, a_0, \ldots, a_{n-1}$. Jest więc spełniony również warunek R2. □

Konstrukcja ta jest szczególnie prosta, gdy G jest grupą cykliczną $\boldsymbol{Z}_n$. Zerowy wiersz zawiera wtedy $\{\infty, 0\}$ w zerowej kolumnie oraz $\{x_1, y_1\}, \ldots, \{x_s, y_s\}$ w kolumnach odpowiednio $-a_1, \ldots, -a_s$. Każdy następny wiersz otrzymujemy przesuwając poprzedni cyklicznie w prawo o jedną pozycję i dodając 1 (modulo n) do każdego elementu ($\infty + 1 = \infty$). Oto dla przykładu kwadrat Rooma odpowiadający starterowi (12.4) i sumatorowi (12.5) w $\boldsymbol{Z}_7$:

	0	1	2	3	4	5	6
0	∞0			25		16	34
1	45	∞1			36		20
2	31	56	∞2			40	
3		42	60	∞3			51
4	62		53	01	∞4		
5		03		64	12	∞5	
6			14		05	23	∞6

Macierz $A = [a_{ij}]$ wymiaru $n \times n$ taką, że $a_{ij} = 0$, jeśli klatka $\langle i, j \rangle$ jest pusta, i $a_{ij} = 1$ w przeciwnym przypadku, nazywamy *macierzą incydencji* kwadratu Rooma. Macierz ta ma $\frac{1}{2}(n+1)$ jedynek w każdym wierszu i każdej kolumnie, może więc odpowiadać pewnej konfiguracji Hadamarda o parametrach $v = 4t-1$, $k = 2t$, $\lambda = t$, gdzie $t = \frac{1}{4}(n+1)$. Jeśli tak jest w istocie, to mówimy, że kwadrat Rooma jest *typu Hadamarda*. Skonstruowany przez nas kwadrat Rooma o boku 7 jest typu Hadamarda – jego macierz incydencji odpowiada konfiguracji dopełnieniowej względem płaszczyzny Fano.

Kwadrat Rooma nazywamy *standardyzowanym*, jeśli jego główna przekątna zawiera – po ewentualnym przenumerowaniu symboli – pary $\{0, 1\}$, $\{0, 2\}, \ldots, \{0, n\}$. Konstrukcja z twierdzenia 12.1 daje zawsze kwadrat standardyzowany i oczywiście z dowolnego kwadratu Rooma można otrzymać kwadrat standardyzowany przez permutację wierszy i kolumn. Standardyzowany kwadrat Rooma nazywamy *skośnym*, jeśli dla dowolnych i, j, $i \neq j$, dokładnie jedna z klatek $\langle i, j \rangle$, $\langle j, i \rangle$ jest pusta. Skonstruowany kwadrat jest skośny.

Zajmiemy się teraz pewnymi szczególnymi typami starterów i sumatorów. Starter $\langle \{x_1, y_1\}, \ldots, \{x_s, y_s\} \rangle$ nazywamy *regularnym*, jeśli $y_i = -x_i$ dla $1 \leqslant i \leqslant s$. Oczywiście, dowolne dwa startery regularne w tej samej grupie nie różnią się istotnie, gdyż fakt, iż pary $\{x_1, y_1\}, \ldots, \{x_s, y_s\}$ są uporządkowane w ciąg, ma znaczenie jedynie dla ustalenia odpowiedniości między parami $\{x_i, y_i\}$ startera i elementami a_i sumatora. Można łatwo sprawdzić, że pary $\{x, -x\}$, $x \neq 0$ istotnie tworzą starter w dowolnej grupie przemiennej rzędu nieparzystego (p. zad. 64).

Niestety są grupy, w których nie istnieje sumator dla startera regularnego, choć istnieje dla pewnego startera nieregularnego. Sprawdzono na przykład za pomocą komputera, że nie istnieje sumator dla startera regularnego w Z_9, choć dla startera

$$\langle \{1, 2\}, \{3, 7\}, \{4, 6\}, \{5, 8\} \rangle \tag{12.6}$$

istnieje sumator

$$\langle 1, 7, 2, 8 \rangle. \tag{12.7}$$

Starter $\langle \{x_1, y_1\}, \ldots, \{x_s, y_s\} \rangle$ nazywamy *silnym*, jeśli wszystkie sumy $x_i + y_i$, $1 \leqslant i \leqslant s$, są różne i niezerowe. Jest to bardzo ważna klasa starterów, ze względu na następującą własność:

LEMAT 12.2. *Jeśli $S = \langle \{x_1, y_1\}, \ldots, \{x_s, y_s\} \rangle$ jest silnym starterem w grupie przemiennej G, to*

$$A = \langle -x_1 - y_1, \ldots, -x_s - y_s \rangle$$

jest sumatorem dla S.

Dowód. Oznaczmy $a_i = -x_i - y_i$. Elementy a_i, $1 \leqslant i \leqslant s$ są różne i niezerowe, przy czym $x_i + a_i = -y_i$, $y_i + a_i = -x_i$. Z definicji startera $\{x_1, \ldots, x_s\} \cup$

$\cup \{y_1, \ldots, y_s\} = G \setminus \{0\}$, zatem

$$\{x_1+a_1, \ldots, x_s+a_s\} \cup \{y_1+a_1, \ldots, y_s+a_s\} =$$
$$= \{-y_1, \ldots, -y_s\} \cup \{-x_1, \ldots, -x_s\}$$
$$= \{-x\colon x \in G \setminus \{0\}\} = G \setminus \{0\},$$

co dowodzi, iż A jest sumatorem dla S. □

Pokażemy teraz pewną konstrukcję silnych starterów pochodzącą od Mullina i Nemetha.

TWIERDZENIE 12.3. *Jeśli p jest liczbą pierwszą różną od 2 oraz $p^m = 2^k t+1$, gdzie t jest nieparzyste i większe od jedności, to istnieje silny starter w grupie addytywnej ciała $GF(p^m)$.*

Dowód. Niech a będzie elementem pierwotnym w $GF(p^m)$. Jeśli oznaczymy $d = 2^{k-1}$, to $a^{2dt} = a^{p^m-1} = 1$ oraz $a^r \neq 1$ dla $1 \leqslant r < 2dt$. Oznaczmy dla $0 \leqslant i \leqslant d-1$, $0 \leqslant j \leqslant t-1$,

$$X_{ij} = \{a^{i+2jd}, a^{i+(2j+1)d}\}.$$

Wykażemy, że tak zdefiniowane dt par X_{ij} tworzy silny starter. Z faktu, iż a jest elementem pierwotnym wynika, że

$$\bigcup_{i=0}^{d-1} \bigcup_{j=0}^{t-1} X_{ij} = \{a^k\colon 0 \leqslant k \leqslant 2dt-1\} = GF(p^m) \setminus \{0\}.$$

Zbadamy teraz różnice

$$a^{i+2jd} - a^{i+(2j+1)d} = a^{i+2jd}(1-a^d), \tag{12.8}$$

$$a^{i+(2j+1)d} - a^{i+2jd} = a^{i+2jd}(a^d-1). \tag{12.9}$$

Mamy $a^d \neq 1$, a więc równość dwóch różnic pierwszego typu,

$$a^{i+2jd}(1-a^d) = a^{i_1+2j_1d}(1-a^d),$$

może zachodzić tylko wtedy, gdy $i+2jd = i_1+2j_1d$, czyli $i = i_1$, $j = j_1$. Podobni nie ma dwóch takich samych różnic drugiego typu. Załóżmy teraz, że pewn różnica pierwszego typu pokrywa się z różnicą drugiego typu, tzn.

$$a^{i+2jd} = a^{i_1+2j_1d}.$$

Mamy wówczas

$$a^{(i-i_1)+2d(j-j_1)} = -1$$

i po podniesieniu obu stron do kwadratu

$$a^{2(i-i_1)+4d(j-j_1)} = 1.$$

Rząd elementu a wynosi $2dt$, ta ostatnia równość oznacza więc, że

$$2(i-i_1)+4d(j-j_1) \equiv 0 \pmod{2dt}. \tag{12.10}$$

Wynika stąd w szczególności, że $i-i_1 \equiv 0 \pmod{d}$. Wobec nierówności $0 \leqslant i$, $i_1 \leqslant d-1$ wnioskujemy, że $i = i_1$. Po uwzględnieniu tej równości kongruencja (12.10) przyjmuje postać

$$4d(j-j_1) \equiv 0 \pmod{2dt}.$$

Mamy stąd $2(j-j_1) \equiv 0 \pmod{t}$ i wobec nieparzystości t ostatecznie $j-j_1 \equiv \equiv 0 \pmod{t}$. Lecz $0 \leqslant j, j_1 \leqslant t-1$, a więc $j = j_1$. Tak więc wszystkie różnice (12.8), (12.9) są różne i niezerowe, co oznacza, że pary X_{ij} określają starter. Element a^d jest różny od -1, gdyż $(a^d)^2 = a^{2d} \neq 1 = a^{2dt}$ (założyliśmy $t > 1$). Wszystkie sumy

$$a^{i+2jd} + a^{i+(2j+1)d} = a^{i+2jd}(1+a^d), \quad 0 \leqslant i \leqslant d-1, \quad 0 \leqslant j \leqslant t-1$$

są więc niezerowe i różne, gdyż niezerowe i różne są elementy a^{i+2jd}, $0 \leqslant i \leqslant d-1$, $0 \leqslant j \leqslant t-1$. Skonstruowany starter jest więc silny. □

WNIOSEK 12.4. *Jeśli p jest liczbą pierwszą różną od 2 oraz p^m-1 nie jest potęgą dwójki, to istnieje kwadrat Rooma o boku p^m.* □

Pełny dowód istnienia kwadratu Rooma o boku n dla dowolnego n, z wyjątkiem $n = 3$ i $n = 5$, jest zbyt skomplikowany by go tu przytoczyć. Warto jednak powiedzieć na czym polega jego idea. Bardzo niedokładnie można by ją przedstawić następująco: Należy wykazać, że (i) dla dowolnej liczby pierwszej p istnieje kwadrat Rooma o boku p, oraz (ii) jeśli istnieją kwadraty Rooma o bokach n i m, to istnieje również kwadrat Rooma o boku nm. Taki schemat dowodu byłby do przyjęcia, gdyby nie fakt, że jego pierwsza część jest fałszywa — nie istnieją kwadraty Rooma o bokach 3 i 5. Co więcej, konstrukcja Mullina i Nemetha opisana w twierdzeniu 12.3 nie gwarantuje istnienia kwadratu Rooma o boku równym liczbie pierwszej postaci 2^k+1. Łatwo wykazać, że liczba 2^k+1 może być pierwsza tylko wtedy, gdy k jest postaci 2^n. Liczby $f_n = 2^{2^n}+1$ znane są w teorii liczb pod nazwą *liczb Fermata*. Liczby $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$ są pierwsze (Fermat przypuszczał, że wszystkie liczby f_n są pierwsze, lecz dziś wiemy, że f_5, f_6, f_7, f_8 są złożone, przy czym nie jest znana żadna liczba pierwsza f_n dla $n \geqslant 5$). Trudności te zostały przezwyciężone przez wykazanie, że dla $n \geqslant 2$ istnieje kwadrat Rooma o boku f_n, oraz przez udowodnienie, że dla dowolnej liczby nieparzystej k istnienie kwadratu Rooma o boku $n > k$ pociąga za sobą istnienie kwadratu Rooma o boku kn (Wallis [1]).

Na zakończenie powróćmy jeszcze do problemu organizowania rozgrywek brydżowych. Wygodnie nam będzie nazywać zespołem każdą parę zawodników uczestniczących w rozgrywkach. Brakującą w kwadracie Rooma informację dotyczącą tego, który zespół ma grać na jakiej linii przy rozgrywaniu każdego rozdania może być dostarczona przez nadanie pewnego uporządkowania każdej parze elementów (tzn. zespołów) występującej w kwadracie Rooma. Możemy się umówić, że pierwszy element takiej uporządkowanej pary wskazuje na zespół, który ma grać na linii NS. Każdej kolumnie kwadratu Rooma możemy przyporządkować dwa zbiory: zbiór złożony z pierwszych elementów oraz zbiór złożony z drugich

elementów par znajdujących się w tej kolumnie. W sumie otrzymujemy $2n$ podzbiorów $A_1, \ldots, A_{2n}$ $\frac{1}{2}(n+1)$-elementowych zbioru $(n+1)$-elementowego zespołów uczestniczących w rozgrywkach. Zwykle stawia się następujące dodatkowe żądanie: Każda para (nieuporządkowana) zespołów jest porównywana w trakcie rozgrywek tę samą liczbę razy, przy czym przez porównanie zespołów rozumiemy rozegranie tego samego rozdania na tej samej linii (zauważmy, że z definicji kwadratu Rooma wynika, że każdy z tych zespołów rozgrywa to rozdanie z innym przeciwnikiem). Warunek ten mówi dokładnie tyle, że zbiory $A_1, \ldots, A_{2n}$ określają konfigurację o parametrach

$$(12.11) \quad v = n+1, \quad k = \tfrac{1}{2}(n+1), \quad b = 2n, \quad r = n, \quad \lambda = \frac{r(k-1)}{v-1} = \tfrac{1}{2}(n-1).$$

Kwadrat Rooma (o uporządkowanych parach elementów) spełniający ten warunek nazywamy *zrównoważonym kwadratem Rooma*. Fakt, że wśród zbiorów $A_1, \ldots, A_{2n}$ każdy zbiór występuje w parze ze swym dopełnieniem, pozwala wyprowadzić następujący warunek konieczny istnienia zrównoważonych kwadratów Rooma:

TWIERDZENIE 12.5 (Parker i Mood [1]). *Jeśli istnieje zrównoważony kwadrat Rooma o boku n, to $n \equiv 3 \pmod 4$, $n > 3$.*

Dowód. Ustalmy pewien zespół x i niech $B_1, \ldots, B_n$ będą tymi spośród zbiorów $A_1, \ldots, A_{2n}$, które zawierają x. Rozważmy dowolne dwa zespoły y, z różne od x. Oznaczmy

$$\begin{aligned} a &= \text{liczba bloków } B_i \text{ takich, że } y, z \in B_i,\\ b &= \text{liczba bloków } B_i \text{ takich, że } y \in B_i,\ z \notin B_i,\\ c &= \text{liczba bloków } B_i \text{ takich, że } y \notin B_i,\ z \in B_i,\\ d &= \text{liczba bloków } B_i \text{ takich, że } y \notin B_i,\ z \notin B_i. \end{aligned}$$

Mamy

$$\begin{aligned} a+b+c+d &= n,\\ a \qquad\quad +d &= \tfrac{1}{2}(n-1) \text{ (liczba zbiorów } A_i \supseteq \{y, z\}\text{; por. (12.11))},\\ a+b \qquad\quad &= \tfrac{1}{2}(n-1) \text{ (liczba zbiorów } A_i \supseteq \{x, y\}),\\ a \quad +c \qquad &= \tfrac{1}{2}(n-1) \text{ (liczba zbiorów } A_i \supseteq \{x, z\}). \end{aligned}$$

Stąd $a = \frac{1}{4}(n-3)$, tzn. $n \equiv 3 \pmod 4$. Oczywiście $n > 3$, gdyż nie istnieje kwadrat Rooma o boku 3. □

Zauważmy, że w dowodzie wyprowadziliśmy następujący warunek, który jest być może silniejszy od warunku $n \equiv 3 \pmod 4$ (zakładamy $n > 3$): Istnieje konfiguracja Hadamarda o parametrach $v = n$, $k = \frac{1}{2}(n-1)$, $\lambda = \frac{1}{4}(n-3)$, lub równoważnie – macierz Hadamarda rzędu $n+1$. Konfiguracja ta jest określona przez podzbiory $B_1 \setminus \{x\}, \ldots, B_n \setminus \{x\}$ zbioru wszystkich zespołów różnych od X.

Zadania

1. Udowodnić, że jeśli istnieją konfiguracje o parametrach v, k, λ oraz v_1, k_1, λ_1 przy czym $v_1 = k$, to istnieje konfiguracja o parametrach v, k_1, $\lambda\lambda_1$.

2. Podać przykład parametrów v, k, λ spełniających zależności (1.9), (1.10), lecz nie spełniających nierówności Fischera (1.11).

3. Udowodnić, że jeśli istnieją konfiguracje o parametrach v, k, λ oraz v, k, λ', to dla dowolnych m, $m' \in N_0$ istnieje konfiguracja o parametrach v, k, $m\lambda + m'\lambda'$.

4. Niech $\mathscr{G} = \{G_1, \ldots, G_n\}$ będzie podziałem zbioru v-elementowego X na podzbiory m-elementowe zwane *grupami*, oraz niech $\mathscr{B} = (B_1, \ldots, B_b)$ będzie rodziną podzbiorów k-elementowych zbioru X zwanych *blokami*. Będziemy mówili, że $\langle X, \mathscr{G}, \mathscr{B} \rangle$ jest *konfiguracją podzielną na grupy* o parametrach v, k, λ, m, jeśli (i) $|G_i \cap B_j| \leqslant 1$ dla $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant b$, oraz (ii) jeśli x, y nie należą do tej samej grupy, to para $\{x, y\}$ zawarta jest dokładnie w λ blokach. Udowodnić, że jeśli istnieje konfiguracja podzielna na bloki o parametrach v, k, λ, $m = k$, to istnieje konfiguracja o parametrach v, k, λ.

5. Udowodnić, że jeśli istnieje konfiguracja podzielna na grupy (por. zadanie poprzednie) o parametrach v, k, λ, $m = k-1$, to istnieje konfiguracja o parametrach $v+1$, k, λ, przy czym w przypadku $\lambda = 1$ prawdziwe jest również twierdzenie odwrotne.

6. Oznaczmy $n = k - \lambda$. Wykazać, że parametr n konfiguracji kwadratowej nie zmienia się przy przejściu do konfiguracji dopełnieniowej, oraz że między parametrami v, n, k, λ dowolnej konfiguracji kwadratowej zachodzą następujące zależności:

$$4n - 1 \leqslant v \leqslant n^2 + n + 1,$$

$$k = \tfrac{1}{2}(v + \varepsilon\sqrt{v^2 - 4vn + 4n}),$$

$$\lambda = \tfrac{1}{2}(v - 2n + \varepsilon\sqrt{v^2 - 4vn + 4n}),$$

gdzie $\varepsilon = -1$ lub $\varepsilon = 1$.

7. Udowodnić, że dla każdego n istnieje tylko skończona liczba nieizomorficznych konfiguracji kwadratowych, których parametry k, λ spełniają równość $k - \lambda = n$.

Wskazówka: Skorzystać z oszacowania parametru v uzyskanego w poprzednim zadaniu.

8 (Ryser). Udowodnić, że jeśli A jest nieosobliwą macierzą rzeczywistą wymiaru $v \times v$ spełniającą zależność

$$AA^T = (k-\lambda)I + \lambda J \quad \text{lub} \quad A^T A = (k-\lambda)I + \lambda J$$

oraz

$$AJ = kJ \quad \text{lub} \quad JA = kJ$$

(k, λ są dowolnymi liczbami rzeczywistymi), to A spełnia wszystkie cztery równania oraz $\lambda(v-1) = k(k-1)$.

9 (Ryser). Udowodnić, że jeśli macierz wymiaru $v \times v$ o współczynnikach całkowitych i nieujemnych sumach kolumn spełnia równanie $AA^T = (k-\lambda)I + \lambda J$, przy czym liczba (k, λ) jest wolna od kwadratów, liczba $k - \lambda$ zaś nieparzysta, to A jest macierzą incydencji konfiguracji kwadratowej.

10. Udowodnić, że każda konfiguracja o parametrach $v = n^2$, $k = n$, $\lambda = 1$, jest konfiguracją resztową dla pewnej jednoznacznie wyznaczonej płaszczyzny rzutowej.

11. Udowodnić, że dla dowolnej $(\lambda - k)$-konfiguracji λRP jest kwadratem liczby całkowitej.

12 (W. G. Bridges). Udowodnić, że dla dowolnej λ-konfiguracji $e_1 \neq 2$.

13. Udowodnić, że 2-konfigurację z rys. 30 można otrzymać z płaszczyzny Fano przez operację uzupełnienia.

14. Udowodnić, że λ-konfiguracja o macierzy incydencji A jest uzupełnieniem pewnej konfiguracji kwadratowej wtedy i tylko wtedy, gdy sumy kolumn macierzy A przyjmują dwie wartości, z których jedna występuje dokładnie raz.

15. Udowodnić, że jeśli $\lambda > 1$, to dla dowolnej λ-konfiguracji $\lambda/(\lambda-1) \leqslant \varrho \leqslant \lambda$.

16. Udowodnić, że zastępując dowolny blok konfiguracji o parametrach $v = 4\lambda - 1$, $k = 2\lambda$, $\lambda \geqslant 2$, przez jego dopełnienie otrzymujemy λ-konfigurację o parametrach $r_1 = 2\lambda+1$, $r_2 = 2\lambda-1$, przy czym każdą λ-konfigurację o tych wartościach r_1, r_2 można otrzymać za pomocą takiej konstrukcji.

17. Podać prosty dowód twierdzenia 3.6 przy założeniu prawdziwości hipotezy opisanej na końcu §3.

18. Wykazać, że nie istnieje konfiguracja kwadratowa o parametrach $v = 22$, $k = 7$, $\lambda = 2$ oraz $v = 46$, $k = 10$, $\lambda = 2$.

19. Niech $b = b_1 + b_2 i + b_3 j + b_4 k$, $x = x_1 + x_2 i + x_3 j + x_4 k$ będą dwoma kwaternionami (p. Sierpiński [1]). Sprawdzić, że $bx = y_1 + y_2 i + y_3 j + y_4 k$, gdzie y_1, y_2, y_3, y_4 są określone przez układ (4.4) (przypomnijmy, że $i^2 = j^2 = k^2 = -1$, $ij = k$, $jk = i$, $ki = j$, $ji = -k$, $kj = -i$, $ik = -j$). Zdefiniujmy *normę kwaternionu* $a = a_1 + a_2 i + a_3 j + a_4 k$ wzorem $N(a) = a_1^2 + a_2^2 + a_3^2 + a_4^2$. Wykazać, że norma iloczynu jest równa iloczynowi norm i wyprowadzić stąd tożsamość (4.3).

20. W dowodzie twierdzenia Brucka–Rysera–Chowli wykazaliśmy, że istnieje rozwiązanie równania (4.1) spełniające warunek $x \neq 0$, gdy $v \equiv 1 \pmod 4$, oraz $z \neq 0$, gdy $v \equiv 3 \pmod 4$. Udowodnić, że warunki te nie stanowią istotnego wzmocnienia twierdzenia.

21. Udowodnić, że jeśli $n = k - \lambda$ jest kwadratem liczby całkowitej, to równość $\lambda(v-1) = k(k-1)$ jest wystarczająca dla istnienia macierzy A wymiaru $v \times v$ o współczynnikach wymiernych spełniającej równanie $AA^T = nI + \lambda J$.

Wskazówka: $A = \sqrt{n}\, I + v^{-1}(k - \sqrt{n})J$.

22. Udowodnić, że dla $\lambda = 1$ warunki twierdzenia Brucka–Rysera–Chowli wraz z równością $\lambda(v-1) = k(k-1)$ są wystarczające dla istnienia macierzy A wymiaru $v \times v$ o współczynnikach wymiernych, spełniającej równanie $AA^T = nJ + \lambda J$.

Wskazówka: Wykazać, że wtedy

$$\sum_{i=1}^{v} L_i^2 = \sum_{i=2}^{v} n(x_i + x_1/n)^2 + (x_2 + \ldots + x_v)^2.$$

23. Udowodnić, że równania (4.14) i (4.15) są równoważne.

24. Sprawdzić, że zbiór

$$\{0001,\ 0010,\ 0100,\ 1000,\ 0011,\ 1100\}$$

jest zbiorem różnicowym w $\boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2 \oplus \boldsymbol{Z}_2$.

25. Udowodnić, że w definicji zbioru różnicowego o parametrach v, k, λ warunek (5.1) można zastąpić przez

$$d_j^{-1} a_i = d.$$

26. Przedstawmy grupę S_3 wszystkich permutacji zbioru trójelementowego przez 1, a, a^2, b, ab, a^2b, gdzie $a^3 = 1$, $b^2 = 1$, $ba^2 = ab$. Udowodnić, że

$$\begin{aligned} D = \{&\langle 1, 1\rangle, \langle 1, b\rangle, \langle b, 1\rangle, \langle b, ab\rangle, \langle ab, b\rangle,\\ &\langle a, a^2\rangle, \langle a, ab\rangle, \langle ab, 1\rangle, \langle ab, a^2b\rangle, \langle a^2b, ab\rangle,\\ &\langle a^2, a\rangle, \langle 1, a^2b\rangle, \langle a^2b, 1\rangle, \langle a^2b, b\rangle, \langle b, a^2b\rangle\} \end{aligned}$$

jest zbiorem różnicowym o parametrach $v = 36$, $k = 15$, $\lambda = 6$ w (nieprzemiennej!) grupie $S_3 \times S_3$.

27. Udowodnić, że

$$D = \{\langle 1, 1\rangle, \langle 2, 2\rangle, \langle 3, 3\rangle, \langle 4, 4\rangle, \langle 5, 5\rangle,$$
$$\langle 0, 1\rangle, \langle 0, 2\rangle, \langle 0, 3\rangle, \langle 0, 4\rangle, \langle 0, 5\rangle,$$
$$\langle 1, 0\rangle, \langle 2, 0\rangle, \langle 3, 0\rangle, \langle 4, 0\rangle, \langle 5, 0\rangle\}$$

jest zbiorem różnicowym w $Z_6 \oplus Z_6$ o parametrach identycznych jak zbiór z poprzedniego zadania.

28. Udowodnić, że nie istnieje nietrywialny zbiór różnicowy z $k = v/2$.

29. Niech $C = [c_{ij}]$ będzie macierzą wymiaru $v \times v$ taką, że $c_{12} = c_{23} = \ldots = c_{v-1,v} = c_{v,1} = 1$ oraz $c_{ij} = 0$ w pozostałych przypadkach, oraz niech $D = \{a_1, \ldots, a_k\} \bmod v$ będzie cyklicznym zbiorem różnicowym. Wykazać, że wówczas $A = C^{a_1} + \ldots + C^{a_k}$ jest macierzą incydencji konfiguracji wyznaczonej przez D.

30. (Ryser [5]). Przez *zbiór prawie różnicowy* o parametrach v, k, λ (v parzyste) rozumiemy dowolny zbiór $\{a_1, \ldots, a_k\} \bmod v$ taki, że każdą niezerową resztę $d \not\equiv 0, v/2 \pmod v$ można otrzymać na dokładnie λ sposobów jako $d \equiv a_i - a_j \pmod v$ oraz nie istnieją a_i, a_j takie, że $a_i - a_j \equiv v/2 \pmod v$. Załóżmy, że istnieje zbiór prawie różnicowy o parametrach v, k, λ. Udowodnić, że wtedy $k-2$ jest kwadratem w przypadku $v \equiv 0 \pmod 4$ oraz k jest kwadratem w przypadku $v \equiv 2 \pmod 4$. Skonstruować kilka zbiorów prawie różnicowych.

31. Udowodnić, że jeśli istnieje zbiór prawie różnicowy (por. zadanie poprzednie) o parametrach v, k, λ, to istnieje zbiór różnicowy o parametrach $v/2$, k, 2λ.

32. Udowodnić, że dla każdego zbioru różnicowego D o parametrach v, k, λ w grupie G zbiór $G \setminus D$ jest zbiorem różnicowym o parametrach $\bar{v} = v$, $\bar{k} = v-k$, $\bar{\lambda} = v-2k+\lambda$, wyznaczającym konfigurację dopełnieniową względem konfiguracji wyznaczonej przez D.

33. Udowodnić, że dla każdej rodziny różnicowej o parametrach v, k, λ, t wzór (7.2) określa konfigurację o parametrach v, k, λ, $r = tk$, $b = tv$.

34. Udowodnić, że parametry rodziny różnicowej spełniają zależność $\lambda(v-1) = tk(k-1)$.

35. Skonstruować zbiór różnicowy

- typu H_6 ($x = 1$, $p = 31$, $r = 3$),
- typu T ($p = 3$, $s = 5$, $r = 2$),
- typu B ($x = 3$),
- typu B_0 ($x = 1$),
- typu O ($a = 3$, $b = 1$),
- typu W_4 ($p = 5$, $r = 3$).

36. Niech p będzie liczbą pierwszą, $q = p^m = 4s+1$ oraz niech a będzie elementem pierwotnym w $GF(q)$. Udowodnić, że

$$(\{a^{2r}\colon 1 \leqslant r \leqslant 2s\}, \{a^{2r+1}\colon 1 \leqslant r \leqslant 2s\})$$

jest rodziną różnicową o parametrach

$$v = 4s+1, \quad k = 2s, \quad \lambda = 2s-1, \quad t = 2$$

w grupie addytywnej ciała $GF(q)$.

37. Udowodnić, że zbiory różnicowe o parametrach $v = 31$, $k = 15$, $\lambda = 7$ typu S (określone przez $PG(4, 2)$) i typu Q (reszty kwadratowe w Z_{31}) są nierównoważne.

38. Podzbiory m-elementowe A, B grupy przemiennej G rzędu $2m+1$ nazywamy *zbiorami różnicowymi Szekeresa*, jeśli (i) $a \in A \Rightarrow -a \notin A$, (ii) (A, B) jest rodziną różnicową w G. Niech x będzie elementem pierwotnym w $GF(q)$, $q = 4m+3$, niech $Q = \{x^{2b}\colon 1 \leqslant b \leqslant 2m+1\}$, oraz niech

$$A = \{b\colon 1 \leqslant b \leqslant 2m+1 \wedge x^{2b}-1 \in Q\},$$
$$B = \{b\colon 1 \leqslant b \leqslant 2m+1 \wedge x^{2b}+1 \in Q\}.$$

Udowodnić, że A, B są zbiorami różnicowymi Szekeresa w Z_{2n+1}. Skonstruować zbiory różnicowe Szekeresa w Z_5.

39. Udowodnić następujące wzmocnienie twierdzenia 8.2: Niech D będzie zbiorem różnicowym o parametrach v, k, λ w grupie przemiennej G, niech $p_1, \ldots, p_s$ będą różnymi liczbami pierwszymi takimi, że $m = p_1, \ldots, p_s$ jest dzielnikiem liczby $n = k-\lambda$. Jeśli $(m, v) = 1$, $m > \lambda$, oraz t jest liczbą całkowitą taką, że $t \equiv p_i^{e_i} \pmod v$ dla odpowiednich potęg $p_i^{e_i}$, $i = 1, \ldots, s$, to t jest mnożnikiem zbioru D.

40. Korzystając z poprzedniego zadania skonstruować cykliczny zbiór różnicowy o parametrach $v = 23$, $k = 11$, $\lambda = 5$ i wykazać, że jest on jedyny.

41. Skonstruować cykliczną płaszczyznę rzutową rzędu 8 i wykazać jej jedyność korzystając z metody mnożników ($p = 2$).

42. Udowodnić, że automorfizm grupy $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$ zdefiniowany następująco:

$$\alpha\colon \langle b_1, b_2, b_3, b_4 \rangle \mapsto \langle b_{\pi(1)}, b_{\pi(2)}, b_{\pi(3)}, b_{\pi(4)} \rangle,$$

gdzie π jest dowolną permutacją zbioru $\{1, 2, 3, 4\}$, ustala zbiór D określony przez (8.14), a więc jest automorfizmem konfiguracji wyznaczonej przez D.

43. Identyfikując $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$ z grupą addytywną ciała $GF(16)$ zbadać, czy istnieje automorfizm tej grupy postaci $x \mapsto xg\,(g \in G)$, który indukowałby automorfizm konfiguracji wyznaczonej przez zbiór (8.14).

44. Udowodnić, że -1 nie jest mnożnikiem żadnego niezdegenerowanego cyklicznego zbioru różnicowego.

45. Uzupełnić dowód lematu 9.6.

46. Skonstruować parę ortogonalnych kwadratów łacińskich rzędu 10.

47. Udowodnić, że jeśli istnieje płaszczyzna rzutowa rzędu n, to $N(n^2+n+1) \geqslant N(n+1)$.

48. Korzystając z poprzedniego zadania udowodnić, że $N(21) \geqslant 4$ i porównać to ograniczenie z wartością otrzymaną z twierdzenia 9.5.

49. Udowodnić, że opisana w tym rozdziale konstrukcja płaszczyzny rzutowej ze zbioru ortogonalnych kwadratów łacińskich o elementach z $GF(q)$ daje płaszczyznę izomorficzną z $PG(2, q)$.

50. Udowodnić następujące własności iloczynu Kroneckera macierzy:
(a) $a(A \times B) = (aA) \times B = A \times (aB)$ (a — skalar),
(b) $(A+B) \times C = (A \times C)+(B \times C)$,
(c) $A \times (B+C) = (A \times B)+(A \times C)$,
(d) $(A \times B)(C \times D) = AC \times BD$,
(e) $(A \times B)^T = A^T \times B^T$,
(f) $(A \times B) \times C = A \times (B \times C)$.
(Zakładamy, że wymiary macierzy A, B, C, D są takie, że wszystkie te wyrażenia mają sens.) Udowodnić lemat 10.4 korzystając z (d) i (e).

51. Macierz Hadamarda jest *regularna*, jeśli suma elementów w każdym wierszu i kolumnie jest stała. Udowodnić, że jeśli H jest macierzą regularną Hadamarda rzędu $4t$ o sumie każdego wiersza i kolumny równej s, to s jest parzyste i $A = \frac{1}{2}(H+J)$ jest macierzą incydencji konfiguracji kwadratowej o parametrach $v = 4t$, $k = 2t+\frac{1}{2}s$, $\lambda = t+\frac{1}{2}s$. Wyprowadzić stąd wniosek, iż jeśli istnieje macierz regularna Hadamarda rzędu $4t$, to t jest kwadratem liczby całkowitej ($t = (\pm\frac{1}{2}s)^2$).

52. Korzystając z wyniku poprzedniego zadania udowodnić, że macierz regularna Hadamarda rzędu $4n^2$ istnieje wtedy i tylko wtedy, gdy istnieje konfiguracja kwadratowa o parametrach $v = 4n^2$, $k = 2n^2+n$, $\lambda = u^2+u$.

53. Macierz H wymiaru $n \times n$ o elementach 1, -1, i, $-$i (i oznacza jednostkę urojoną) nazywamy *macierzą zespoloną Hadamarda* rzędu n, jeśli $HH^* = nI$, gdzie H^* oznacza macierz sprzężoną z H, tzn. powstałą z H^T przez zamianę każdego elementu na element sprzężony. Udowodnić, że rząd macierzy

zespolonej Hadamarda jest równy 1 lub jest liczbą parzystą (przypuszcza się, że istnieją macierze zespolone Hadamarda dowolnego rzędu parzystego).

54. Skonstruować macierz zespoloną Hadamarda rzędu 6.

55. Niech C będzie macierzą zespoloną Hadamarda rzędu c, H zaś macierzą (rzeczywistą) Hadamarda rzędu h. Niech

$$R = I_{h/2} \times \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},$$

gdzie $I_{h/2}$ jest macierzą jednostkową wymiaru $(h/2)\times(h/2)$, $K = HR$ oraz niech $C = X+\mathrm{i}Y$, gdzie X, Y są macierzami rzeczywistymi. Udowodnić, że $(X\times H)+(Y\times K)$ jest macierzą (rzeczywistą) Hadamarda rzędu ch.

56. Udowodnić następujące twierdzenie Williamsona [1]: Niech S będzie macierzą wymiaru $n\times n$ taką, że $S^T = \varepsilon S$, $\varepsilon = \pm 1$, $SS^T = (n-1)I_n$, oraz niech A, B będą macierzami wymiaru $m\times m$ takimi, że

$$AA^T = BB^T = mI_m, \qquad AB^T = -\varepsilon BA^T.$$

Wówczas macierz $K = (A\times I_n)+(B\times S)$ spełnia warunek $KK^T = mnI_{mn}$.

57. Korzystając z wyniku poprzedniego zadania udowodnić następujące twierdzenie uogólniające drugą konstrukcję Paley'a: Jeśli $q \equiv 1 \pmod 4$ jest potęgą liczby pierwszej oraz istnieje macierz Hadamarda rzędu $n > 1$, to istnieje macierz Hadamarda rzędu $n(q+1)$.

Wskazówka: Przyjmujemy za A dowolną macierz Hadamarda rzędu n oraz

$$B = \left(I_{n/2} \times \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right) A.$$

58. Sprawdzić, że (11.5) przedstawia płaszczyznę Fano.

59. Udowodnić, że proste w $AG(n, q)$ określają konfigurację rozwiązywalną o parametrach $v = q^n$, $k = q$, $\lambda = 1$ (por. (6.8)). W szczególności, dla $q = 3$ otrzymujemy system trójek Kirkmana rzędu 3^n.

60. Sprawdzić, że (11.6) odpowiada systemowi trójek Kirkmana izomorficznemu z systemem określonym przez proste w $AG(2, 3)$.

61 (R. C. Bose). Udowodnić, że dla dowolnej konfiguracji rozwiązywalnej o parametrach v, k, λ, b, r zachodzi nierówność $b \geqslant v+r-1$.

62. Niech S_1, S_2 będą systemami trójek Steinera odpowiednio na zbiorach $\{x_1, \ldots, x_{v_1}\}$, $\{y_1, \ldots, y_{v_2}\}$, i rozważmy zbiór X składający się z $v_1 v_2$ elementów z_{ij}, $1 \leqslant i \leqslant v_1$, $1 \leqslant j \leqslant v_2$. Niech S będzie rodziną podzbiorów zbioru X złożoną z trójek $\{z_{ir}, z_{js}, z_{kt}\}$ takich, że

(i) $r = s = t$ i $\{x_i, x_j, x_k\}$ jest trójką systemu S_1, lub

(ii) $i = j = k$ i $\{y_r, y_s, y_t\}$ jest trójką systemu S_2, lub

(iii) $\{x_i, x_j, x_k\}$ jest trójką systemu S_1 i $\{y_r, y_s, y_t\}$ jest trójką systemu S_2.

Udowodnić, że S jest systemem trójek Steinera rzędu $v_1 v_2$.

63. Udowodnić, że nie istnieje kwadrat Rooma o boku 5.

64. Udowodnić, że pary $\{x, -x\}$, $x \in G\setminus\{0\}$ tworzą regularny starter w dowolnej grupie przemiennej G rzędu nieparzystego.

65. Sumator $\langle a_1, \ldots, a_s\rangle$ jest *skośny*, jeśli $a_i \neq -a_j$ dla wszelkich i, j, $1 \leqslant i, j \leqslant s$. Udowodnić, że w przypadku startera skośnego konstrukcja opisana w twierdzeniu 12.1 daje skośny kwadrat Rooma.

66. Skonstruować kwadrat Rooma o boku 9 odpowiadający starterowi (12.6) i sumatorowi (12.7).

67. Przez *faktor* grafu o $2k$ wierzchołkach rozumiemy zbiór k krawędzi grafu, z których żadne dwie nie zawierają tego samego wierzchołka. *Faktoryzacją* grafu nazywamy podział zbioru jego krawędzi na

pewną liczbę faktorów. Dwie faktoryzacje $\mathscr{F}_1$, $\mathscr{F}_2$ są ortogonalne, jeśli każde dwa faktory $F_1 \in \mathscr{F}_1$, $F_2 \in \mathscr{F}_2$ zawierają co najwyżej jedną wspólną krawędź. Jaki jest związek między kwadratami Rooma o boku n a ortogonalnymi faktoryzacjami grafu pełnego K_{n+1}?

68. Udowodnić, że sumator otrzymany w konstrukcji Mullina i Nemetha (twierdzenie 12.3) jest skośny.

69. Udowodnić, że jeśli $p^m > 3$ jest potęgą nieparzystej liczby pierwszej oraz $p \equiv 3 \pmod 4$, to istnieje zrównoważony kwadrat Rooma o boku p^m.

Wskazówka: Zastosować konstrukcję z twierdzenia 12.3.

ROZDZIAŁ 8

KODY KORYGUJĄCE BŁĘDY

§ 1. Ogólne zasady kodowania i dekodowania

W trakcie przesyłania danych na łączach komunikacyjnych powstają błędy. Związane to jest z różnymi zjawiskami fizycznymi. Prawdopodobieństwo powstawania takich błędów w trakcie transmisji nie będzie nas tu zajmować.

Opiszmy ogólny schemat kodowania i odkodowywania danych. Mamy zatem pewną daną, przedstawioną zazwyczaj w postaci ciągu zero-jedynkowego, którą przesyłamy w łączu. Jednakże w trakcie transmisji wystąpić mogą błędy i zamiast nadanego słowa $\boldsymbol{a}$ otrzymamy inne słowo $B(\boldsymbol{a})$. Sytuacja ta zmusza nas do przedsięwzięcia kroków zabezpieczających przekaz. Postępujemy w następujący sposób: Słowu $\boldsymbol{a}$ przypisujemy dłuższe słowo $K(\boldsymbol{a})$. Słowo to powinno mieć następującą własność: Jeśli w trakcie transmisji wystąpiło „mało” błędów i otrzymaliśmy słowo $B(K(\boldsymbol{a}))$, to mamy metodę odtworzenia zeń słowa $K(\boldsymbol{a})$ i — w konsekwencji — słowa $\boldsymbol{a}$. Znaczenie słowa „mało” zależy oczywiście od użytego kodu.

Podajmy bardzo prosty przykład. Przesyłamy słowa binarne długości 5. Słowo $\langle a_1, \ldots, a_5\rangle$ kodujemy w następujący sposób $\langle a_1, a_1, a_1, a_2, a_2, a_2, \ldots, a_5, a_5, a_5\rangle$. Kod taki nazywamy kodem trzykrotnie powtarzającym. Umówimy się, że „mało” oznacza, iż w trakcie transmisji, w kolejno wysyłanych grupach trzyliterowych, wystąpi nie więcej niż jeden błąd. Funkcja K przekształca w naszym przypadku $(GF(2))^5$ w $(GF(2))^{15}$. Nadaliśmy zatem ciąg $\langle b_1, \ldots, b_{15}\rangle$ a otrzymaliśmy ciąg $\langle c_1, \ldots, c_{15}\rangle$. Jak odtworzyć zeń nasz oryginalny ciąg? Dzielimy ciąg $\langle c_1, \ldots, c_{15}\rangle$ na 5 grup $\langle c_1, c_2, c_3\rangle$, $\langle c_4, c_5, c_6\rangle, \ldots, \langle c_{13}, c_{14}, c_{15}\Leftarrow$. W każdej z grup znajdujemy element, który występuje 2 lub 3 razy. Rozważmy na przykład $\langle c_7, c_8, c_9\rangle$. Jeśli wystąpił tam co najwyżej jeden błąd, to należy zastąpić ciąg $\langle c_7, c_8, c_9\rangle$ ciągiem stałym, którego wyrazem jest ten powtarzający się element. Odtwarzamy w ten sposób ciąg $\langle b_1, \ldots, b_{15}\rangle$, a stąd już łatwo znaleźć $\langle a_1, \ldots, a_5\rangle$.

Wiedząc teraz jakie jest nasze zadanie wprowadzimy podstawowe definicje. Niech A będzie zbiorem skończonym zwanym *alfabetem*, zaś $n\in N$. *Odległością*

Hamminga słów $\boldsymbol{a} = \langle a_1, \ldots, a_n \rangle$ i $\boldsymbol{b} = \langle b_1, \ldots, b_n \rangle$ w A^n nazywamy liczność zbioru $\{i\colon a_i \neq b_i\}$. Liczbę tę oznaczamy $d_H(\boldsymbol{a}, \boldsymbol{b})$. Łatwo sprawdzić, iż funkcja d_H spełnia aksjomaty metryki:

(a) $d_H(\boldsymbol{a}, \boldsymbol{b}) = 0$ wtedy i tylko wtedy gdy $\boldsymbol{a} = \boldsymbol{b}$,

(b) $d_H(\boldsymbol{a}, \boldsymbol{b}) = d_H(\boldsymbol{b}, \boldsymbol{a})$,

(c) $d_H(\boldsymbol{a}, \boldsymbol{b}) \leqslant d_H(\boldsymbol{a}, \boldsymbol{c}) + d_H(\boldsymbol{c}, \boldsymbol{b})$;

$d_H(\boldsymbol{a}, \boldsymbol{b})$ to nic innego jak liczba błędów, które zostały popełnione, jeśli nadano słowo $\boldsymbol{a}$, odebrano zaś $\boldsymbol{b}$. Oprócz korekcji błędów – zadania, które opisywaliśmy powyżej – mamy też zadanie detekcji błędów, mianowicie wykrycia, czy błąd (błędy) wystąpił(y), przy założeniu, że błędów jest mało. Powszechnie stosowana w transmisji danych binarnych jest tzw. *kontrola parzystości*. Niech dany będzie ciąg binarny $\boldsymbol{a} = \langle a_1, \ldots, a_n \rangle$. Niech $K(\boldsymbol{a})$ będzie ciągiem długości $n+1$ określonym jak następuje:

$$K(\boldsymbol{a}) = \langle a_1, \ldots, a_n, \delta \rangle, \qquad \text{gdzie } \delta = (a_1 + \ldots + a_n) (\mathrm{mod}\, 2).$$

Jeśli $\langle b_1, \ldots, b_{n+1} \rangle = K(\boldsymbol{a})$, to zgodnie z konstrukcją

$$\sum_{j=1}^{n} b_j \equiv 0 \,(\mathrm{mod}\, 2).$$

Jeśli „mało” oznacza „co najwyżej jeden” to po przesłaniu $K(\boldsymbol{a})$ z małą liczbą błędów jesteśmy w stanie albo stwierdzić, że błędów nie ma i odkodować $\boldsymbol{a}$ (mianowicie, jeśli suma otrzymanego ciągu jest parzysta, pomijamy po prostu ostatni wyraz ciągu), albo też stwierdzić, że błąd gdzieś wystąpił i zasygnalizować to zdarzenie. W ten sposób *wykryliśmy* błąd choć nie *skorygowaliśmy* go. Zauważmy, że schemat kodowania – a więc para $\langle K, D \rangle$, gdzie $D = K^{-1}$ – może mieć różne zdolności korekcji i wykrywania. Na przykład schemat polegający na sześciokrotnym kolejnym powtórzeniu każdej litery kodowej koryguje popełnienie co najwyżej dwóch a wykrywa popełnienie co najwyżej trzech błędów w każdej grupie kodowej. W dalszym ciągu naszych rozważań będziemy zajmowali się sytuacją, w której:

(1) wszystkie słowa kodowane mają tę samą długość k,

(2) wszystkie słowa kodowe mają tę samą długość n,

(3) każde słowo alfabetu A długości n niesie informację.

Tak więc $K\colon A^k \to A^n$, $D\colon A^n \to A^k$, przy czym $DK = I_{A^k}$ (identyczność na A^k).

Najczęściej rozważamy przypadek $A = \{0, 1\}$, odpowiednie zaś kody nazywamy *binarnymi*.

Wagą słowa $\boldsymbol{a}$ nazwijmy $w(\boldsymbol{a}) = d_H(\boldsymbol{a}, \boldsymbol{0})$ (gdzie $\boldsymbol{0} = \langle 0, \ldots, 0 \rangle$). $(GF(2))^n$ ma strukturę przestrzeni liniowej nad $GF(2)$. Odległość Hamminga $d_H(\boldsymbol{a}, \boldsymbol{b})$ jest równa w naszym przypadku $w(\boldsymbol{a} + \boldsymbol{b})$. Określmy jeszcze pojęcie *kuli* o *promieniu* d i środku w $\boldsymbol{a}$, oznaczanej przez $S_d(\boldsymbol{a})$, jak następuje:

$$S_d(\boldsymbol{a}) = \{\boldsymbol{b}\colon d_H(\boldsymbol{a}, \boldsymbol{b}) \leqslant d\}.$$

Jeśli $\boldsymbol{b} \notin S_d(\boldsymbol{a})$, to popełnienie w trakcie przekazywania $\boldsymbol{a}$ co najwyżej d błędów nie spowoduje otrzymania słowa $\boldsymbol{b}$. Z uwagi tej wynika natychmiast następujący fakt:

TWIERDZENIE 1.1. *Na to, by kod wykrywał fakt popełnienia w trakcie przesyłania słów kodujących co najwyżej d błędów, potrzeba i wystarcza, by dla dowolnych słów kodowych* $\boldsymbol{a}$ *i* $\boldsymbol{b}$

$$\boldsymbol{a} \neq \boldsymbol{b} \Rightarrow \boldsymbol{a} \notin S_d(\boldsymbol{b}). \quad \square$$

W przypadku gdy chcemy korygować – a nie tylko wykrywać błędy – sytuacja jest bardziej skomplikowana. Jeśli popełnimy co najwyżej d błędów w trakcie transmisji słowa $\boldsymbol{a}$ i zbliżymy się na odległość nie większą niż d do słowa $\boldsymbol{b}$, to nie jesteśmy w stanie stwierdzić, które ze słów było nadawane. Tak się jednak nie stanie dokładnie w jednym przypadku: jeśli dla dowolnych słów kodowych ich odległość wynosi co najmniej $2d+1$. Wtedy bowiem – zgodnie z warunkiem trójkąta – odejście od $\boldsymbol{a}$ na odległość k nie spowoduje zbliżenia się do $\boldsymbol{b}$ na odległość mniejszą albo równą $d+1$. Dowiedliśmy w ten sposób równie oczywistego następującego faktu:

TWIERDZENIE 1.2. *Na to, by kod korygował popełnienie w trakcie przesyłania słów kodujących co najwyżej d błędów, potrzeba i wystarcza, by dla dowolnych słów kodowych* $\boldsymbol{a}$ *i* $\boldsymbol{b}$

$$\boldsymbol{a} \neq \boldsymbol{b} \Rightarrow d_H(\boldsymbol{a}, \boldsymbol{b}) \geqslant 2d+1. \quad \square$$

Zbiór słów kodowanych (gdy $A = GF(2)$) jest obdarzony strukturą przestrzeni liniowej. W dalszym ciągu często będziemy zajmowali się sytuacją, gdy funkcja K jest różnowartościowym odwzorowaniem liniowym $(GF(2))^k$ w $(GF(2))^n$. Sytuacja taka ma mnóstwo zalet; jedną z nich jest to, że wystarczy znać wartości K na bazie przestrzeni $(GF(2))^k$.

Odwzorowanie K może być zadane macierzą wymiaru $k \times n$ rzędu k.

Rozważmy na przykład następującą macierz wymiaru 2×4:

$$\boldsymbol{K} = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Słowu kodowanemu $\langle 1, 0 \rangle$ przyporządkowujemy więc słowo $\langle 1, 1, 0, 1 \rangle$, słowu zaś $\langle 0, 1 \rangle$ słowo $\langle 1, 0, 1, 0 \rangle$; ogólnie: wektorowi $\boldsymbol{a}$ przyporządkowujemy wektor $K(\boldsymbol{a}) = \boldsymbol{a} \cdot \boldsymbol{K}$. Odwzorowanie nasze jest różnowartościowe, bowiem obrazy wektorów z bazy są liniowo niezależne. $\square$

Tak więc, jeśli słowa kodowe określone są za pomocą wzoru $K(\boldsymbol{a} = \boldsymbol{a} \cdot \boldsymbol{K}$, gdzie K jest rzędu k to tworzą one n-wymiarową przestrzeń liniową nad ciałem $GF(2)$. W tej sytuacji kod nasz (czyli obraz zbioru $(GF(2))^k$) nazywamy (n, k)-*kodem liniowym*.

Takie właśnie kody będziemy badali poniżej. Oczywiście wektor $\boldsymbol{0}$ należy do dowolnej podprzestrzeni przestrzeni $(GF(2))^k$, a zatem w naszej sytuacji $\boldsymbol{0}$ jest zawsze słowem kodowym.

Udowodnimy najpierw kilka prostych faktów dotyczących binarnych kodów liniowych. Zauważmy najpierw, że minimalna odległość słów kodowych jest równa minimalnej wadze słowa kodującego. Istotnie, mamy w naszej sytuacji $d_H(\boldsymbol{a}, \boldsymbol{b}) = w(\boldsymbol{a}+\boldsymbol{b}) = d_H(\boldsymbol{a}+\boldsymbol{b}, \boldsymbol{0})$. Jeśli nadane zostało słowo $\boldsymbol{a}$, otrzymane zaś $\boldsymbol{b}$, to różnicę $\boldsymbol{b}-\boldsymbol{a}$ (w naszym przypadku jest to także $\boldsymbol{a}+\boldsymbol{b}$) będziemy nazywali *błędem*. W ten sposób wektor $\boldsymbol{e}$ wyznacza nam warstwę względem kodu C mianowicie $C+\boldsymbol{e}$. Niestety, $\boldsymbol{e}$ nie jest jedynym wektorem wyznaczającym warstwę. Łatwo widać, że jeśli $\boldsymbol{a}$ jest słowem kodowym, to $\boldsymbol{e}+\boldsymbol{a}$ i $\boldsymbol{e}$ wyznaczają tę samą warstwę.

Wybierzmy w każdej warstwie element, który nazwiemy *liderem* tej warstwy. Zauważmy, że każda warstwa liczy dokładnie tyle samo elementów, co kod C, a więc 2^k elementów. Mamy zatem $2^n/2^k = 2^{n-k}$ warstw. Wybrawszy w każdej warstwie W jej lidera $\boldsymbol{e}_W$, a następnie ustaliwszy jakikolwiek porządek kodu C (w którym $\boldsymbol{0}$ jest pierwszym elementem) i warstw, otrzymujemy macierz, której wyrazami są słowa długości 2^n, powstającą jak następuje: w pierwszym wierszu wypisujemy nasze słowa kodowe, a w pierwszej kolumnie liderów warstw. Dalej ustalamy

$$\boldsymbol{a}_{ij} = \boldsymbol{e}_{W_i} + \boldsymbol{a}_j,$$

gdzie $\boldsymbol{e}_{W_i}$ jest liderem i-tej warstwy, $\boldsymbol{a}_j$ zaś j-tym słowem kodowym. Całą tę macierz nazywamy *słownikiem* kodu.

Przy ustalonym słowniku reguła korygowania jest następująca: „Znaleźć kolumnę, w której występuje otrzymane słowo, i wypisać element z pierwszego wiersza tej kolumny".

Teraz już opisana metoda jest jasna; przyjmujemy mianowicie, że najbardziej prawdopodobnym spośród błędów „produkujących" warstwę W jest jej lider, i korygujemy błąd tak, że odejmujemy $\boldsymbol{e}_W$ od otrzymanego słowa. Oczywiście, kandydatem na lidera warstwy jest — zgodnie z tą interpretacją — słowo w warstwie o minimalnej wadze (mianowicie odpowiada to błędowi po nadaniu słowa $\boldsymbol{0}$). Element taki nie musi być w warstwie jedyny.

Rozważmy nasz kod zadany macierzą

$$E = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

Słowa kodowe są następujące:

$$\langle 0, 0, 0, 0\rangle, \quad \langle 1, 1, 0, 1\rangle, \quad \langle 1, 0, 1, 0\rangle, \quad \langle 0, 1, 1, 1\rangle.$$

Pozostałe trzy warstwy mają postać:

$$\langle 1, 0, 0, 0\rangle, \quad \langle 0, 1, 0, 1\rangle, \quad \langle 0, 0, 1, 0\rangle, \quad \langle 1, 1, 1, 1\rangle,$$
$$\langle 0, 1, 0, 0\rangle, \quad \langle 1, 0, 0, 1\rangle, \quad \langle 1, 1, 1, 0\rangle, \quad \langle 0, 0, 1, 1\rangle,$$
$$\langle 0, 0, 0, 1\rangle, \quad \langle 1, 1, 0, 0\rangle, \quad \langle 1, 0, 1, 1\rangle, \quad \langle 0, 1, 1, 0\rangle.$$

Zauważmy, że jedynie w pierwszej warstwie mieliśmy dwóch kandydatów na liderów.

W przypadku, gdy $A = GF(2)$, a nawet ogólniej, gdy $A = GF(q)$, mamy następujące eleganckie kryterium znajdowania lidera w warstwie. Określmy dla $\boldsymbol{a}, \boldsymbol{b} \in (GF(q))^n$ relację $\prec$ wzorem

$$\boldsymbol{a} \prec \boldsymbol{b} \Leftrightarrow (a_i = b_i \vee a_i = 0) \quad \text{dla } i = 1, \ldots, n.$$

Określmy w każdej warstwie następujący porządek: Liczby ciała $GF(q)$ uporządkowane są tak, że liczby różne od zera ustawiamy zgodnie z porządkiem w N, liczbę $\mathbf{0}$ stawiamy na końcu (w $GF(2)$ porządek ten to 1, 0, w $GF(5)$ 1, 2, 3, 4, 0). Porządkujemy teraz elementy o minimalnej wadze leksykograficznie — zgodnie z tym porządkiem. Pierwszy element wybieramy jako lidera. (Postąpiliśmy tak w powyższym przykładzie.) Zachodzi wtedy

TWIERDZENIE 1.3. *Jeśli $\boldsymbol{a}$ jest liderem warstwy i $\boldsymbol{b} \prec \boldsymbol{a}$, to $\boldsymbol{b}$ też jest liderem.*

Dowód. $\boldsymbol{b} \prec \boldsymbol{a}$ oznacza, że w $\boldsymbol{a}$ zmniejszyliśmy co najwyżej liczbę wyrazów niezerowych. Wystarczy wykazać, że zastępując w $\boldsymbol{a}$ kolejno wyrazy niezerowe zerami otrzymujemy w dalszym ciągu liderów. Oczywiście, wystarczy to wykazać w sytuacji, gdy zmniejszamy liczbę wyrazów niezerowych w $\boldsymbol{a}$ o jeden. Mamy wówczas $w(\boldsymbol{a}-\boldsymbol{b}) = 1$.

Słowa kodowe z $C+\boldsymbol{a}$ powstają ze słów z $C+\boldsymbol{b}$ poprzez dodawanie $\boldsymbol{a}-\boldsymbol{b}$. Ponieważ słowa z $C+\boldsymbol{a}$ mają wagę nie mniejszą niż waga $\boldsymbol{a}$ ($\boldsymbol{a}$ jest bowiem liderem o minimalnej wadze), więc słowa w $C+\boldsymbol{b}$ nie mogą mieć wagi mniejszej niż $w(\boldsymbol{b})$. Gdyby bowiem $\boldsymbol{c} \in C+\boldsymbol{b}$ i $w(\boldsymbol{c}) < w(\boldsymbol{b})$, to $\boldsymbol{c}+\boldsymbol{a}-\boldsymbol{b} \in C+\boldsymbol{a}$ oraz $w(\boldsymbol{c}+\boldsymbol{a}-\boldsymbol{b}) \leqslant w(\boldsymbol{c})+w(\boldsymbol{a}-\boldsymbol{b}) = w(\boldsymbol{c})+1 < w(\boldsymbol{b})+1 = w(\boldsymbol{a})$, wbrew temu, że $\boldsymbol{a}$ jest liderem. Zatem $w(\boldsymbol{b})$ jest minimalna w całej warstwie $C+\boldsymbol{b}$.

Wektor $\boldsymbol{e} = \boldsymbol{a}-\boldsymbol{b}$ ma dokładnie jedną pozycję niezerową e_k. Wybierzmy lidera $\boldsymbol{l}$ warstwy $C+\boldsymbol{b}$ zgodnie z powyższymi regułami. Słowo $\boldsymbol{l}+\boldsymbol{e}$ ma wagę minimalną w $C+\boldsymbol{a}$. Gdyby $l_k \neq 0$, to waga $\boldsymbol{l}+\boldsymbol{e}$ mogłaby tylko się utrzymać lub ulec zmniejszeniu o jeden w stosunku do wagi $\boldsymbol{l}$. Tak nie jest (waga została powiększona), zatem $l_k = 0$. Teraz już wystarczy sprawdzić, że jeśli $\boldsymbol{l} \neq \boldsymbol{b}$, to $\boldsymbol{l}+\boldsymbol{e}$ jest leksykograficznie po $\boldsymbol{a}$, a zatem $\boldsymbol{l}$ jest leksykograficznie po $\boldsymbol{b}$. □

Skoro słowa kodowe, elementy przestrzeni C, tworzą przestrzeń nad ciałem (powiedzmy $GF(2)$), to mamy naturalnie określony iloczyn skalarny. To z kolei prowadzi do rozważania tzw. *kodu dualnego* $C^{\perp}$. Jest to mianowicie przestrzeń ortogonalna do przestrzeni C, tj. przestrzeń złożona z wektorów $\boldsymbol{d}$ takich, że dla dowolnego $\boldsymbol{a} \in C$

$$\boldsymbol{a} \cdot \boldsymbol{d} = 0.$$

Twierdzenia algebry liniowej nad ciałami o charakterystyce 0 nie przenoszą się *verbatim* na przypadek przestrzeni nad ciałami o charakterystyce skończonej. W szczególności nie musi być prawdą, iż $C \cap C^{\perp} = \{0\}$.

Kodowi C możemy przypisać macierz, której wierszami są wektory tworzące bazę przestrzeni C (macierz taka nie jest zatem jedyna). Macierz taką nazywamy *macierzą generującą kod* C. Macierz przestrzeni ortogonalnej do przestrzeni C nazywamy *macierzą kontroli parzystości*.

Jeśli dane są dwa kody C_1 i C_2, to mówimy, że są one *równoważne*, jeśli istnieje permutacja π taka, że $\langle a_1, \ldots, a_n \rangle \in C_1 \Leftrightarrow \langle a_{\pi(1)}, \ldots, a_{\pi(n)} \rangle \in C_2$. Łatwo widać, że dla każdego kodu C istnieje równoważny mu kod D, którego macierz generująca ma postać

$$[I_k E] = \begin{bmatrix} 1 & 0 & & 0 & \ldots \\ 0 & 1 & & 0 & \ldots \\ & & \ddots & & \\ 0 & 0 & & 1 & \ldots \end{bmatrix}.$$

Zachodzi następujące twierdzenie:

TWIERDZENIE 1.4. *Jeśli $[I_k P]$ jest macierzą generującą kod C, to macierz $[-P^T)I_{n-k}]$ jest macierzą kontroli parzystości dla C.*

Dowód tego twierdzenia podamy dla sytuacji, gdy kod C jest podprzestrzenią przestrzeni $(GF(2))^n$. Wykażemy najpierw, że wiersze macierzy $[I_k P]$ są prostopadłe do wierszy macierzy $[-P^T I_{n-k}]$. W tym celu narysujmy następujący diagram:

$$\begin{matrix} I_k & P \\ & I_{n-k} \end{matrix}$$

Musimy wykazać, że wiersze macierzy $[I_k P]$ są prostopadłe do kolumn macierzy $\begin{bmatrix} P \\ I_{n-k} \end{bmatrix}$. Wykażemy to przez indukcję ze względu na liczbę niezerowych elementów w macierzy P. Niech zatem P' powstaje z P przez wprowadzenie jedynki na miejsce $p_{i_0 j_0}$, $1 \leqslant i_0 \leqslant k$, $n-k \leqslant j_0 \leqslant n$. Oznaczmy wiersze starej macierzy $[I_n P]$ przez w_i (a nowej macierzy $[I_k P']$ przez w_i') oraz kolumny macierzy $\begin{bmatrix} P \\ I_{n-k} \end{bmatrix}$ przez v_j (a nowej macierzy przez v_j').

Założenie indukcyjne jest następujące:

$$w_i \cdot v_j = 0.$$

Mamy

$$w_i' = \begin{cases} w_i, & i \neq i_0, \\ w_i + e_{j_0}, & i = i_0. \end{cases}$$

Podobnie

$$v_j' = \begin{cases} v_j, & j \neq j_0, \\ v_j + e_{i_0}, & j = j_0. \end{cases}$$

Wtedy jednak $w_i' \cdot v_j' = 0$, jeśli $i \neq i_0 \wedge j \neq j_0$.

Pozostają do rozpatrzenia trzy przypadki: $i \neq i_0 \wedge j = j_0$, $i = i_0 \wedge j \neq j_0$ oraz $i = i_0 \wedge j = j_0$. Rozpatrzymy trzeci z nich, pierwsze dwa zostawiając do rozważenia Czytelnikowi. Mamy wówczas

$$(w_{i_0} + e_{j_0}) \cdot (v_{j_0} + e_{i_0}) = (v_{i_0} \cdot w_{j_0}) + (e_{j_0} \cdot e_{i_0}) + (w_{i_0} \cdot e_{i_0}) + (v_{j_0} \cdot e_{j_0}).$$

Pierwsze dwa człony są zerami na mocy założenia indukcyjnego i konstrukcji. Oba pozostałe człony są jedynkami. To kończy dowód prostopadłości obu przestrzeni. Jednakże łatwo wykazać, że przestrzeń ortogonalna ma wymiar $n-k$. Istotnie, niech b będzie wektorem prostopadłym do C, niezależnym od wierszy macierzy $[-P^T \; I_{n-k}]$. Wówczas, dodając doń odpowiednią kombinację liniową pierwszych $m-n$ wierszy, możemy „wyredukować" ostatnich $n-k$ wyrazów b do zera. Otrzymany wektor b' powinien być nadal prostopadły do $[I_n \; P]$. Jednakże, jeśli $b_i \neq 0$, to $w_i \cdot b = 1$. Liniowo niezależny układ złożony z wierszy macierzy $[-P^T \; I_{n-k}]$ rozpina przestrzeń $C^{\perp}$, jest zatem jej bazą. □

Teraz już możemy wytłumaczyć, dlaczego macierz generującą dla $C^{\perp}$ nazywamy macierzą kontroli parzystości. Mianowicie opisana powyżej metoda detekcji jednego błędu polega na obraniu kodu takiego, że jego macierz kontroli parzystości składa się z jednego wiersza złożonego z samych jedynek. Odpowiada temu równanie spełnione przez słowa kodujące: $a_1 + \ldots + a_n = 0$.

Zatem macierz kontroli parzystości to nic innego jak skrócony zapis tego, że słowa kodujące to wszystkie rozwiązania pewnego jednorodnego układu równań. Jeśli

$$H = \begin{bmatrix} h_{11} & \ldots & h_{1n} \\ \ldots & \ldots & \ldots \\ h_{k1} & \ldots & h_{kn} \end{bmatrix},$$

to słowa kodowe są rozwiązaniami układu:

$$\begin{gathered} h_{11}a_1 + \ldots + h_{1n}a_n = 0, \\ \ldots\ldots\ldots\ldots\ldots \\ h_{k1}a_1 + \ldots + h_{kn}a_n = 0; \end{gathered}$$

symbolicznie zapisujemy to jak następuje:

$$a \in C \Leftrightarrow a \cdot H^T = \mathbf{0}.$$

W ten sposób uzyskamy pełną informację o kodzie liniowym C, jeśli mamy bądź jego macierz generującą, bądź macierz kontroli parzystości. Zauważmy jeszcze, że jeśli W jest warstwą, to wszystkie elementy W dają przy mnożeniu przez H^T ten sam wektor, zwany czasem *objawem* W (różne warstwy dają różne objawy).

Kod C mający macierz tworzącą postaci $[I_k \; P]$ (a więc i macierz kontroli parzystości postaci $[-P^T \; I_{n-k}]$) nazywamy *zredukowanym*. W przypadku kodu zredukowanego każde słowo kodowane $\langle a_1, \ldots, a_k \rangle$ rozszerza się jednoznacznie do słowa kodowego poprzez dodanie na końcu $n-k$ symboli służących do ewentualnej detekcji lub korekcji.

§ 2. Kody doskonałe, kod Hamminga

Jak pamiętamy z poprzedniego paragrafu, warunkiem na to, by kod korygował e błędów, jest, aby dla dowolnych słów kodowych a i b, $a \neq b \Rightarrow S_e(a) \cap S_e(b) = \emptyset$.

To jednak, że kule o środkach w słowach kodowych i o promieniu e są parami

rozłączne, nie oznacza, iż wypełniają one przestrzeń słów. Mogą — *a priori* — istnieć słowa, które odległe są od każdego słowa kodowego o co najmniej $e+1$. Jeśli taka sytuacja nie może się zdarzyć, to kod nasz nazywamy doskonałym. Tak więc mamy następującą definicję.

Kod V korygujący e błędów nazywamy *kodem doskonałym*, jeśli $\bigcup_{a \in V} S_e(a) = A^m$.

Skonstruujemy teraz kod doskonały korygujący jeden błąd. Kod ten został znaleziony przez Hamminga. Niech k będzie liczbą naturalną. Liczby $1, \ldots, 2^k-1$ możemy zapisać w dwójkowym układzie pozycyjnym dopełniając „z przodu" otrzymane ciągi zerami tak, by otrzymać ciągi długości k. Niech wreszcie macierz H wymiaru $k \times (2^k-1)$ będzie macierzą powstałą z kolejnego wypisania skonstruowanych ciągów. Macierz H jest macierzą kontroli parzystości konstruowanego kodu. Łatwo widać, że skonstruowany kod jest $(2^k-1, 2^k-k-1)$-kodem (a więc słowa kodowane mają długość 2^k-k-1, słowa kodowe długość 2^k-1). Wykażemy, że skonstruowany kod jest doskonały. W tym celu wykażemy najpierw, że kod nasz koryguje jeden błąd. Jest tak, ponieważ wszystkie kolumny macierzy kontroli parzystości są różne i niezerowe. Zatem pojedynczy błąd, powiedzmy w j-tej kolumnie, powoduje, że w wyniku pomnożenia słowa otrzymanego przez macierz H^T otrzymujemy j-tą kolumnę macierzy H (zauważmy w tym miejscu, że objawem jest zawsze suma kolumn odpowiadających miejscom, w których popełniliśmy błędy). Tak więc kod nasz koryguje jeden błąd. Co więcej, z powyższej uwagi wynika metoda korekcji: otrzymane słowo mnożymy przez macierz H^T. W wyniku powstaje wektor będący rozwinięciem liczby naturalnej z przedziału $0, \ldots, 2^k-1$. Jeśli otrzymaliśmy liczbę 0, to (zgodnie z założeniem, które mówi, że popełniliśmy co najwyżej jeden błąd) nie popełniliśmy błędu. Jeśli otrzymaliśmy liczbę $j > 0$, to w badanym słowie b należy na j-tej współrzędnej zastąpić b_j przez $1-b_j$.

Aby wykazać, że kod Hamminga jest doskonały, zauważmy, że słowo kodowane ma długość 2^k-k-1, słowo kodowe zaś ma długość 2^k-1. Słów kodowanych (a zatem kodowych) jest $2^{(2^k-k-1)}$, wszystkich zaś słów otrzymywanych jest $2^{(2^k-1)}$. Ponieważ każda kula o promieniu 1 liczy dokładnie 2^k elementów (słowo kodowe oraz dokładnie 2^k-1 słów odległych odeń o 1, pamiętamy bowiem, że długość słowa kodującego wynosi 2^k-1), wystarczy skorzystać z równości $2^{2^k-1} = 2^k \cdot (2^{2^k-k-1})$, by zobaczyć, że kod nasz jest doskonały.

Kod Hamminga może być uogólniony na przypadek alfabetów innych niż $GF(2)$. Nie będziemy jednak wnikali w tę konstrukcję, a jedynie przedstawimy (15, 11)-kod Hamminga (tj. dla $k = 4$). Ma on — zgodnie z powyższą konstrukcją — następującą macierz kontroli parzystości:

$$\begin{bmatrix} 0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&0&1&1&1&1&0&0&0&0&1&1&1&1 \\ 0&1&1&0&0&1&1&0&0&1&1&0&0&1&1 \\ 1&0&1&0&1&0&1&0&1&0&1&0&1&0&1 \end{bmatrix},$$

Transpozycje kolumn (1, 15), (2, 14), (4, 13) i (8, 12) prowadzą nas do kodu równoważnego, którego macierz kontroli parzystości jest następująca:

$$\begin{bmatrix} 1&1&0&1&0&0&0&1&1&1&1&1&0&0&0 \\ 1&1&0&1&1&1&1&1&0&0&0&0&1&0&0 \\ 1&1&1&0&0&1&1&0&0&1&1&0&0&1&0 \\ 1&0&1&1&1&0&1&0&1&0&1&0&0&0&1 \end{bmatrix}.$$

Macierzą generującą dla tego kodu jest

$$\begin{bmatrix} 1&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \\ 0&1&0&0&0&0&0&0&0&0&0&1&1&1&0 \\ 0&0&1&0&0&0&0&0&0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&0&0&0&0&0&1&1&0&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&1&1&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&1&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&1&1&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&1&0&0&1 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0 \\ 0&0&0&0&0&0&0&0&0&0&1&1&0&1&1 \end{bmatrix}.$$

Wykonując permutację odwrotną na kolumnach naszej macierzy otrzymujemy:

$$\begin{bmatrix} 1&1&0&1&0&0&0&1&0&0&0&0&0&0&1 \\ 0&1&0&1&0&0&0&1&0&0&0&0&0&1&0 \\ 1&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&0&1&0&0&0&1&0&0&0&0&1&0&0 \\ 1&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&1&0&0&1&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0 \\ 1&0&0&0&0&0&0&1&1&1&0&0&0&0&0 \\ 0&1&0&0&0&0&0&1&0&1&0&0&0&0&0 \\ 1&1&0&0&0&0&0&1&0&0&1&0&0&0&0 \end{bmatrix}.$$

Po przekształceniach otrzymujemy następującą macierz generującą kodu Hamminga:

$$\begin{bmatrix}
1&0&0&0&0&0&0&0&0&0&0&1&0&0&1\\
0&1&0&0&0&0&0&0&0&0&0&1&1&0&1\\
0&0&1&0&0&0&0&0&0&0&0&1&1&1&1\\
0&0&0&1&0&0&0&0&0&0&0&1&1&1&0\\
0&0&0&0&1&0&0&0&0&0&0&0&1&1&1\\
0&0&0&0&0&1&0&0&0&0&0&1&0&1&0\\
0&0&0&0&0&0&1&0&0&0&0&0&1&0&1\\
0&0&0&0&0&0&0&1&0&0&0&1&0&1&1\\
0&0&0&0&0&0&0&0&1&0&0&1&1&0&0\\
0&0&0&0&0&0&0&0&0&1&0&0&1&1&0\\
0&0&0&0&0&0&0&0&0&0&1&0&0&1&1
\end{bmatrix}.$$

W przypadku, gdy używany przez nas alfabet A, $|A| = q$, nie jest obdarzony strukturą ciała, a mimo to chcemy wybrać zbiór słów kodowych $C \subseteq A^n$ tak, by kod nasz korygował jeden błąd i był kodem doskonałym, to rozumowanie użyte w dowodzie doskonałości kodu Hamminga daje następujący wniosek: Skoro kula $S_1(\boldsymbol{a})$ liczy dokładnie $1+n(q-1)$ wektorów (bo zliczając wektory z $S_1(\boldsymbol{a})$ mamy do wyboru $\boldsymbol{a}$ oraz, dla każdej z n współrzędnych, $q-1$ wektorów różniących się od $\boldsymbol{a}$ na j-ej współrzędnej), to mamy, o ile taki kod istnieje,

$$1+n(q-1) | q^n.$$

Jest to oczywiście warunek konieczny. Zauważmy jednakże, że jeśli q jest potęgą liczby pierwszej, powiedzmy $q = p^m$, to $1+n(q-1) = p^r$ dla pewnego r. Wykażemy, że wówczas $1+n(q-1) = q^a$ dla pewnego a.

Jeśli tak nie jest, to $1+n(q-1) = p^j q^b$, gdzie $j < m$, wtedy zaś po przekształceniu

$$n = \frac{p^j q^b - 1}{q-1} = p^j \frac{q^b-1}{q-1} + \frac{p^j - 1}{q-1}.$$

Jednakże $(p^j - 1)/(q-1)$ nie jest liczbą całkowitą, zaś n i $(q^b-1)/(q-1)$ są, co jest niemożliwe.

Dla wykazania, że nasz warunek nie jest warunkiem wystarczającym, rozważmy $n = 7$, $q = 6$. Wówczas $1+n(q-1) = 36 = 6^2$, oraz $6^2 | 6^7$. Załóżmy, że $V \subseteq \{1, \ldots, 6\}^7$ jest kodem doskonałym korygującym jeden błąd. Kod nasz liczy 6^5 słów (gdyż sfera $S_1(\boldsymbol{a})$ liczy 36 elementów). Jeśli dwa słowa kodowe $\langle a_1, \ldots, a_7 \rangle$ i $\langle b_1, \ldots, b_7 \rangle$ mają identycznych pierwszych 5 pozycji, to ich odległość jest równa 2, co wyklucza korekcję błędu. Zatem hipotetyczny kod V ma tę własność, że

odcinki początkowe długości 5 słów kodowych są różne, i skoro kod liczy 6^5 słów, wyczerpują $\{1, \ldots, 6\}^5$. Ustalmy a, b, c i rozważmy zbiór wszystkich słów kodowych zaczynających się od $\langle a, b, c\rangle$. Słów tych jest 36 (mianowicie dla $i, j \in \{1, \ldots, 6\}$ mamy dokładnie jedno słowo zaczynające się od $\langle a, b, c, i, j\rangle$). Rozważmy zatem słowa $\langle a, b, c, i, j, a_{ij}, b_{ij}\rangle$ należące do naszego kodu. Skoro naszych 36 słów ma odległość Hamminga co najmniej równą trzy, to macierze $[a_{ij}]$ oraz $[b_{ij}]$ wymiaru 6×6 są kwadratami łacińskimi (por. rozdział 7, § 9). Istotnie, jeśli i jest ustalone i jeśli $a_{ij_1} = a_{ij_2}$, to odległość naszych ciągów jest co najwyżej 2. Podobnie dla ustalonego j i następnie dla macierzy $[b_{ij}]$. Gdyby dla pewnych par $\langle i_1, j_1\rangle \neq \langle i_2, j_2\rangle$, $\langle a_{i_1j_1}, b_{i_1j_1}\rangle = \langle a_{i_2j_2}, b_{i_2j_2}\rangle$, to znowu odległość odpowiednich ciągów byłaby co najwyżej 2. Tak więc macierze $[a_{ij}]$ i $[b_{ij}]$ byłyby ortogonalne. Taka para — jak wiemy — jednak nie istnieje. To oczywiście kończy dowód.

§ 3. Kody cykliczne, kody BCH

W paragrafie tym rozważymy kody o własności cykliczności, tj. takie kody, które przechodzą na siebie przy zastosowaniu cyklicznej permutacji $\begin{pmatrix}1, 2, \ldots, n-1, n\\ 2, 3, \ldots, n, \quad 1\end{pmatrix}$. W tym celu wprowadzamy reprezentację kodów za pomocą wielomianów. Niech $R = GF(q)[x]$ będzie pierścieniem wielomianów jednej zmiennej, i niech I będzie ideałem głównym generowanym przez wielomian $x^n - 1$. Pierścień ilorazowy, R/I, składa się z klas abstrakcji relacji $f \sim g$ zdefiniowanej wzorem $f \sim g \Leftrightarrow x^n - 1 | f - g$. Każda klasa abstrakcji zawiera dokładnie jeden wielomian stopnia mniejszego niż n. Tak więc możemy pierścień R/I reprezentować jako pierścień wielomianów stopnia mniejszego niż n ze zwykłym dodawaniem i mnożeniem „modulo $x^n - 1$". Mnożenie przez wielomian x odpowiada przekształceniu ciągu współczynników wielomianu w sposób cykliczny: $(a_0 + \ldots + a_{n-1}x^{n-1})x$ jest równy (w naszym pierścieniu) $a_{n-1} + a_0x + \ldots + a_{n-2}x^{n-1}$. Oczywiście, wielomiany z pierścienia R/I z operacją dodawania tworzą przestrzeń liniową izomorficzną z przestrzenią $(GF(q))^n$. W ten sposób podaliśmy wielomianową reprezentację słów używanych do kodowania.

Będziemy mówili, że kod liniowy $C \subseteq (GF(q))^n$ jest *cykliczny* wtedy i tylko wtedy, gdy dla dowolnego $\langle a_1, \ldots, a_n\rangle \in C$, $\langle a_n, a_1, \ldots, a_{n-1}\rangle$ także należy do C.

Kod C — poprzez naszą interpretację — wyznacza podzbiór X_C zawarty w R/I. Warunkiem koniecznym i dostatecznym na to, by C był kodem cyklicznym, jest, by X_C był ideałem w R/I. Istotnie, jeśli C jest kodem cyklicznym, to ilekroć $f \in X_C$, to także $xf \in X_C$. Stąd także x^2f, x^3f etc. należą do X_C. Skoro jednak C był kodem liniowym, to suma elementów z C jest w C, a zatem, jak łatwo widać, suma wielomianów z X_C też należy do C. Zatem, dla dowolnego wielomianu $q(x)$, $q \cdot f \in X_C$ (gdyż $q = a_0 + a_1x + \ldots + a_kx^k$, a wtedy $qf = a_0f + a_1xf + \ldots + a_kx^kf$).

Zatem X_C jest ideałem. Odwrotnie, jeśli X_C jest ideałem, to $f \in X_C$ implikuje, że $xf \in X_C$, co właśnie oznacza cykliczność.

Zauważmy, że R/I jest pierścieniem ideałów głównych (gdyż R jest pierścieniem ideałów głównych). Każdy ideał J w R/I jest więc wyznaczony przez (jedyny) wielomian unormowany najmniejszego stopnia w J. Wielomian taki jest dzielnikiem $x^n - 1$. Zajmiemy się teraz konstrukcją pewnego specjalnego kodu cyklicznego, korygującego zadaną liczbę błędów. Niech d będzie liczbą naturalną, r zaś liczbą naturalną taką, że $q^r \geqslant d+1$. Niech $\alpha \in GF(q^r)$ będzie elementem pierwotnym $GF(q^r)$, a więc elementem, którego rząd multyplikatywny wynosi $q^r - 1$. Niech $w_i(x)$ będzie wielomianem minimalnym dla potęgi α^i (o współczynnikach z ciała $GF(q)$; istnienie takiego wielomianu wykazane jest w Dodatku). Niech $v(x)$ będzie najmniejszą wspólną wielokrotnością wielomianów $w_1(x)$, $w_2(x), \ldots, w_{d-1}(x)$. Ideał generowany przez $v(x)$ wyznacza nam kod cykliczny (ze słowami długości $q^r - 1$) o odległości Hamminga między słowami $\geqslant d$ (zatem korygującym $\lfloor (d-1)/2 \rfloor$ błędów). Kod ten nazywamy *kodem BCH* o projektowanej odległości d. Wykażemy mianowicie następujące twierdzenie.

TWIERDZENIE 3.1 (Bose i Ray-Chaudhuri [1], Hocquenghem [1]). *Dla każdego kodu BCH o projektowanej odległości d odległość (różnych) słów kodowych wynosi co najmniej d.*

Dowód. Na początek zauważmy, że $\alpha, \alpha^2, \ldots, \alpha^{d-1}$ są pierwiastkami $v(x)$, przy czym $v(x)$ jest wielomianem najmniejszego stopnia o tej własności (jeśli bowiem $h(\alpha^k) = 0$, to $w_k | h$). Skoro słowa kodowe są elementami ideału generowanego przez $v(x)$, to każde słowo kodowe przyjmuje dla $\alpha, \alpha^2, \ldots \alpha^{d-1}$ wartość 0. Wykażemy teraz, że każdy wielomian będący słowem kodowym ma nie mniej niż d współczynników niezerowych. To już wystarczy, ponieważ nasz kod jest liniowy i, jak pokazaliśmy uprzednio, odległość minimalna pomiędzy słowami jest równa minimalnej wadze słowa niezerowego.

Przypuśćmy, że $k(x)$ ma mniej niż d współczynników niezerowych, zaś α, $\alpha^2, \ldots, \alpha^{d-1}$ są pierwiastkami $k(x)$. Niech zatem $k(x) = b_1^{n_1} + \ldots + b_{d-1} x^{n_{d-1}}$. Wówczas, podstawiając do k kolejno $\alpha, \alpha^2, \ldots, \alpha^{d-1}$, mamy układ równań liniowych

$$\sum_{j=1}^{d-1} \alpha^{rn_j} b_j = 0, \qquad r = 1, \ldots, d-1$$

(traktujemy teraz b_j jako „niewiadome").

Jeśli wykażemy, że wyznacznik macierzy współczynników jest różny od zera, to — ponieważ układ nasz jest jednorodny — będziemy mieli dokładnie jedno rozwiązanie: $b_j = 0$, $1 \leqslant j \leqslant d-1$. Ale wyznacznik macierzy $[\alpha^{rn_j}]$ wymiaru $(d-1) \times (d-1)$ jest wyznacznikiem typu Vandermonde'a, tj. postaci

$$\begin{vmatrix} s_1 & s_1^2 & \ldots & s_1^{d-1} \\ \ldots & \ldots & \ldots & \ldots \\ s_{d-1} & s_{d-1}^2 & \ldots & s_{d-1}^{d-1} \end{vmatrix}.$$

Wiadomo (por. np. Mostowski i Stark [1], str. 106), że wyznacznik Vandermonde'a jest równy

$$\prod_{i>j} (s_i - s_j).$$

W naszym przypadku jest to

$$\prod_{i>j} (\alpha^{n_i} - \alpha^{n_j}), \qquad i, j = 1, \ldots, d-1.$$

Ale α było elementem rzędu $q^r - 1$, zatem wszystkie elementy α^{n_i}, α^{n_j} są różne (dla $i > j$), wyznacznik jest niezerowy i wszystkie b_j są zerami, co kończy dowód. □

Wykażemy, że kod BCH, gdzie $d = 2$ (tj. wielomian kodujący jest wielomianem minimalnym dla α, gdzie α jest elementem pierwotnym), jest równoważny kodowi Hamminga. Niech zatem $n = 2^m - 1$ i niech α będzie elementem pierwotnym. Wielomian minimalny dla α, zgodnie z wynikami Dodatku, ma postać

$$w_1(x) = (x-\alpha)(x-\alpha^2) \ldots (x-\alpha^{2^{n-1}}).$$

Stopień wielomianu w_1 jest równy n. Ponieważ każdy element x ciała $GF(2^m)$ ma reprezentację

$$x = \sum_{i=0}^{m-1} \varepsilon_i \alpha^i \qquad (\varepsilon_i \in GF(2)),$$

zatem macierz H, której kolumnami są współczynniki rozwinięć obiektów $1 (= \alpha^0)$, $\alpha, \alpha^2, \ldots, \alpha^{2^m - 1}$, ma wszystkie kolumny różne. Jednakże, jeśli słowo $\boldsymbol{a}$ jest równe $\langle a_0, \ldots, a_{n-1} \rangle$, to $\boldsymbol{a}$ jest reprezentowane przez wielomian:

$$a(x) = \sum_{j=0}^{n-1} a_j x^j.$$

Iloczyn $\boldsymbol{a} \cdot H^T$ jest wektorem długości m. Zbadajmy, jak wygląda jego i-ta współrzędna. Jest ona sumą

$$\sum_{j=0}^{n-1} a_j \varepsilon_j^i.$$

Stąd wynika, że otrzymany objaw jest rozwinięciem elementu $a(\alpha)$. Zatem $\boldsymbol{a}$ jest elementem kodu wtedy i tylko wtedy, gdy $a(\alpha) = 0$, czyli $w_1(x) | a(x)$. Skoro macierz kontroli naszego kodu ma wszystkie możliwe kolumny niezerowe długości m, to kod nasz jest $(2^{m-1}, 2^m - m - 1)$-kodem Hamminga, co kończy dowód. □

Zbadajmy efektywność kodów binarnych BCH. W tym celu zauważmy, że użyteczność kodów zależy od tego, ile spośród symboli słowa kodowego niesie informację, ile zaś służy do kontroli. W przypadku kodów BCH mamy następujące

TWIERDZENIE 3.2. *Istnieje kod BCH o słowach kodowych długości $2^m - 1$ i z minimalną (nieparzystą) odległością d, w którym liczba symboli kontrolnych jest nie większa niż $\lfloor (d-1)/2 \rfloor m$.*

Dowód. Zbadajmy dokładniej (w przypadku $q = 2$) wielomian minimalny dla elementu pierwotnego α. Jeśli mianowicie $w(\alpha) = 0$, to $w(\alpha^2) = w(\alpha^4) = \ldots = w(\alpha^{2^i}) = 0$. Podobnie wielomian minimalny dla α^3 zeruje się w α^6. Ogólnie, jeśli $2k \leqslant d-1$, to $w_k(\alpha^{2k}) = 0$. Ale stopień wielomianu w_i (minimalnego dla α^i) jest nie większy niż m, gdyż $\alpha^i \in GF(2^m)$. Stąd najmniejsza wspólna wielokrotność rozważanych wielomianów dzieli iloczyn $(d-1)/2$ z tych wielomianów, zatem ma stopień co najwyżej $\lfloor (d-1)/2 \rfloor m$ (nieparzystość d została użyta). □

W praktyce stosuje się na przykład kod BCH będący (255, 231)-kodem. Kod ten ma minimalną odległość 7, a zatem koryguje 3 a wykrywa 6 błędów. Otrzymuje się go za pomocą elementu pierwotnego α w $GF(256)$. Rząd α jest równy 255. Wielomian użyty do generacji kodu ma stopień 24, jego pierwiastkami są zaś $\alpha, \ldots, \alpha^6$.

Skonstruujemy teraz algorytm odkodowywania dla kodów BCH. Nie będzie on tak prosty, jak w szczególnym przypadku kodów Hamminga. Niemniej istnieją stosunkowo proste metody realizacji poniższego algorytmu za pomocą tzw. rejestrów przesuwnych.

Przypuśćmy zatem, że zadane zostało słowo (reprezentowane jako wielomian) $f(x) = a_{n-1}x^{n-1} + \ldots + a_0$, otrzymane zaś zostało słowo $g(x) = b_{n-1}x^{n-1} + \ldots + b_0$. Słowa f nie znamy, wiemy jedynie, że popełniliśmy nie więcej niż $\lfloor (d-1)/2 \rfloor$ błędów. Oznacza to, że słowo $h(x) = c_{n-1}x^{n-1} + \ldots + c_0$ będące popełnionym błędem, tj. różnicą pomiędzy wielomianami $f(x)$ i $g(x)$, ma nie więcej niż $e \leqslant \lfloor (d-1)/2 \rfloor$ współczynników niezerowych.

Niech α będzie elementem użytym do konstrukcji kodu; innymi słowy liczby α, $\alpha^2, \ldots, \alpha^{d-1}$ są pierwiastkami wielomianu $f(x)$. Zatem, skoro $g(x) = f(x) + h(x)$, mamy:

(3.1) $$h(\alpha^{1+i}) = g(\alpha^{1+i}), \qquad i = 0, \ldots, d-2.$$

Przyjmijmy

$$S_i = g(\alpha^{1+i}), \qquad i = 0, \ldots, d-2.$$

Liczby S_i są nam znane. Na ich podstawie oraz tego, że popełniliśmy co najwyżej $\lfloor (d-1)/2 \rfloor$ błędów, musimy odtworzyć wielomian h. Szukamy więc wielomianu h o co najwyżej $\lfloor (d-1)/2 \rfloor$ niezerowych współczynnikach, dla którego

$$S_i = h(\alpha^{1+i}), \qquad i = 0, \ldots, d-2.$$

Kiedy już taki wielomian znajdziemy, trzeba wykazać, iż jest on jedyny.

Przypuśćmy zatem, że popełniono e błędów, $e \leqslant \lfloor (d-1)/2 \rfloor$ i że wystąpiły one na pozycjach $n_1, \ldots, n_e$. Zatem

$$h(x) = \sum_{j=1}^{e} V_j x^{n_j}$$

(V_j to po prostu c_{n_j} — przyjmujemy ten zapis dla uproszczenia.) Ponieważ

$$h(\alpha^{1+i}) = S_i, \qquad i = 0, \ldots, d-2,$$

więc

$$S_i = \sum_{j=1}^{e} V_j \alpha^{(1+i)n_j}, \qquad i = 0, \ldots, d-2.$$

Przyjmując teraz $\alpha^{n_j} = u_j$ mamy

(3.2) $$S_i = \sum_{j=1}^{e} V_j u_j^{1+i}, \qquad i = 0, \ldots, d-2.$$

Zauważmy, że gdybyśmy otrzymali u_j ($j = 1, \ldots, e$), to ze względu na to, że rząd α wynosi $q^r - 1$, u_j wyznacza n_j, a stąd już znajdujemy V_j jako rozwiązanie układu równań liniowych (3.2). (W przypadku binarnym sytuacja jest jeszcze prostsza, V_j jest po prostu równe 1.) W ten sposób znamy h, a więc i f jako $g-h$.

Dla znalezienia u_j ($j = 1, \ldots, e$) zastosujemy metodę funkcji tworzących. Mianowicie ciągi $\langle u_j \rangle_{j=1}^{e}$ i $\langle V_j \rangle_{j=1}^{e}$ wyznaczają nam, zgodnie ze wzorem (3.2), ciąg nieskończony $\langle S_i \rangle_{i=1}^{\infty}$. Niech $S(x)$ będzie funkcją tworzącą tego ciągu:

$$S(x) = \sum_{i=0}^{\infty} S_i x^i.$$

Dokonując podstawienia zgodnie ze wzorem (3.2) otrzymujemy

$$S(x) = \sum_{i=0}^{\infty} \Big(\sum_{j=1}^{e} v_j u_j^{1+i} \Big) x^i.$$

Zmieniając porządek sumowania otrzymujemy

$$S(x) = \sum_{j=1}^{e} v_j u_j \sum_{i=0}^{\infty} (u_j x)^i.$$

Ale

$$\sum_{i=0}^{\infty} (u_j x)^i = \frac{1}{1-u_j x},$$

a zatem

$$S(x) = \sum_{j=1}^{e} \frac{v_j u_j}{1-u_j x}.$$

Rozważmy teraz wielomian

$$\sigma(x) = \prod_{j=1}^{e} (1-u_j x).$$

Wielomian ten ma stopień e, przy czym jego wyraz wolny jest równy 1.

Mamy teraz

$$S(x)\sigma(x) = \sum_{j=1}^{e} \Big(v_j u_j \prod_{\substack{i=1 \\ i \neq j}}^{e} (1-u_i x) \Big).$$

Stąd też szereg formalny $S(x)\sigma(x)$ jest wielomianem, i to stopnia co najwyżej $e-1$.

Wielomian σ zawiera całą informację o liczbach u_j a więc i o wielomianie h. Obiekty $u_j (j = 1, \ldots, e)$ są mianowicie odwrotnościami pierwiastków wielomianu σ.

Niech zatem $A(x) = \sigma(x)S(x)$. Jak wykazaliśmy, $A(x)$ jest wielomianem stopnia co najwyżej $e-1$, co oznacza, iż szereg formalny $\sigma(x)S(x)$ ma współczynniki o numerach powyżej $e-1$ równe zeru. W szczególności jest tak dla współczynników o numerach $e, e+1, \ldots, d-2$.

Zobaczmy zatem co oznacza „zerowanie się" tych współczynników. Po prostu zachodzą następujące równości:

$$\begin{aligned} &\sigma_0 S_e + \sigma_1 S_{e-1} + \ldots + \sigma_e S_0 = 0, \\ &\sigma_0 S_{e+1} + \sigma_1 S_e + \ldots + \sigma_e S_1 = 0, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\sigma_0 S_{d-2} + \sigma_1 S_{d-3} + \ldots + \sigma_e S_{d-2-e} = 0 \end{aligned} \tag{3.3}$$

(gdzie $\sigma(x) = \sigma_e x^e + \sigma_{e-1} x^{e-1} + \ldots + \sigma_0 = 0$).

Układ (3.3) zdaje się być układem równań liniowych jednorodnych, jednakże nim nie jest, σ_e jest bowiem równe 1. Mamy zatem $d-2-e$ równań liniowych z e niewiadomymi. Znajdujemy obiekty $\sigma_1, \ldots, \sigma_e$ rozwiązujące układ (3.3), następnie rozwiązujemy równanie $\sigma(x) = 0$. Odwrotności pierwiastków są równe szukanym wartościom u_j. Należałoby stwierdzić istnienie i jednoznaczność otrzymanego rozwiązania.

Istnienie rozwiązania jest oczywiste. Kod nasz koryguje bowiem $\lfloor (d-1)/2 \rfloor$ błędów, stąd też istnieje wielomian h spełniający warunki (3.1), a mający co najwyżej $\lfloor (d-1)/2 \rfloor$ współczynników niezerowych.

Dla wykazania jednoznaczności wykażemy następujące twierdzenie:

TWIERDZENIE 3.3. *Wielomian $\sigma(x)$ o współczynnikach będących rozwiązaniem układu* (3.3) *ma najmniejszy stopień spośród wielomianów niezerowych τ stopnia $\lfloor (d-1)/2 \rfloor$ spełniających warunek*

$$\deg(S(x)\tau(x)) \leqslant \lfloor (d-1)/2 \rfloor. \tag{3.4}$$

Co więcej, jest on jedynym z dokładnością do proporcjonalności wielomianem tego stopnia spełniającym warunek (3.4).

Dowód. Niech τ będzie wielomianem możliwie najniższego stopnia e' spełniającym warunek (3.4). Zatem $e' \leqslant e$ i zgodnie z warunkiem (3.4)

$$\sum_{j=0}^{e'} \tau_j S_{i-j} = 0, \quad i = e', \ldots, d-2.$$

Podstawiając S_{i-j} zgodnie z (3.1) mamy

$$\sum_{j=0}^{e'} \tau_j \sum_{k=1}^{e} v_k u_k^{1+i-j} = 0, \qquad i = e', \ldots, d-2.$$

Zmieniamy porządek sumowania otrzymując:

$$\sum_{k=1}^{e} v_k u_k^{1+i} \left(\sum_{j=0}^{e'} \tau_j u_k^{-j} \right), \qquad i = e', \ldots, d-2.$$

Suma w nawiasie jest równa $\tau(u_k^{-1})$ otrzymujemy więc

$$\sum_{k=1}^{e} v_k \tau(u_k^{-1}) u_k^{1+i} = 0, \qquad i = e', \ldots, d-2. \tag{3.5}$$

Potraktujmy (3.5) jako układ równań o niewiadomych $m_k = v_k \tau(u_k^{-1})$. Mamy więc $(d-2)-(e'-1)$ równań wiążących $m_k (k = 1, \ldots, e)$. Skoro $e' \leqslant e \leqslant \lfloor (d-1)/2 \rfloor$, liczba równań jest większa albo równa liczbie niewiadomych. Pierwszych e spośród nich ma niezerowy wyznacznik (jest to bowiem wyznacznik typu Vandermonde'a i wystarczy pamiętać czym są wartości u_j, by stwierdzić, że jest on różny od zera). Stąd też wnosimy, że układ (3.5) ma – w zmiennych m_k – jedynie rozwiązanie zerowe. Oznacza to jednak że

$$V_j \tau(u_j^{-1}) = 0, \qquad j = 1, \ldots, e.$$

Ale $V_j \neq 0$ (gdyż są to wartości błędów). Stąd też

$$\tau(u_j^{-1}) = 0, \qquad j = 1, \ldots, e,$$

co oznacza, że stopień τ musi być co najmniej równy e (gdyż τ ma e różnych pierwiastków), a więc $e' = e$. Ten sam warunek implikuje, że τ i σ są proporcjonalne. □

W ten sposób rozważania nasze zostały zakończone; rozwiązanie istnieje i jest jedyne.

§ 4. Zastosowanie macierzy Hadamarda do konstrukcji kodów korygujących błędy

Przypomnijmy (por. rozdział 7, § 10), że macierzą Hadamarda nazywamy macierz kwadratową H wymiaru $n \times n$ o wyrazach $+1$ i -1 taką, że $H \cdot H^T = nI$. Z takiej macierzy H wygenerujemy kod (niekoniecznie liniowy) binarny o następujących parametrach: Słów kodowych będzie $2n$, słowa kodowe będą miały długość n, odległość minimalna słów kodowych wyniesie $n/2$ (przypomnijmy, że istnienie macierzy Hadamarda o wymiarach $n \times n$, $n > 2$, pociąga za sobą $n \equiv 0 \pmod 4$)). Lematy o istnieniu macierzy Hadamarda (por. rozdział 7, § 10) dają nam w ten sposób natychmiast metodę konstrukcji kodów binarnych rozmaitej odległości.

Niech H będzie macierzą Hadamarda rzędu n. Niech $w_1, w_2, \ldots, w_n$ będą wierszami macierzy H, $v_1, \ldots, v_n$ zaś niech będą odpowiednio równe $-w_1, \ldots$ $\ldots, -w_n$. Zastąpmy teraz w każdym z wektorów $w_1, \ldots, w_n, v_1, \ldots, v_n$ każdy

symbol -1 symbolem 0. Otrzymamy w ten sposób $2n$ wektorów $s_1, \ldots, s_{2n}$, każdy długości n. Wykażemy, że odległość Hamminga s_i i s_j $(i<j)$ jest równa co najmniej $n/2$. Możliwe są trzy przypadki

(1) $i<j\leqslant n$,

(2) $j=i+n$,

(3) $i<n, j=j'+n, i<j'$.

(Pozostałe przypadki: $n<i<j$ oraz $i<n$, $j=j'+n$, $j'<i$ redukują się odpowiednio do (1) i (3).)

(1) Jeśli $i<j\leqslant n$, to $d_H(s_i, s_j) = d_H(w_i, w_j) = n/2$, bowiem iloczyn skalarny w_i i w_j jest równy 0, co oznacza, że na $n/2$ pozycjach wektory w_i i w_j zgadzają się, a na $n/2$ różnią się. Istotnie, wymnażając wyrazy w_i przez odpowiadające im wyrazy wektora w_j otrzymujemy w przypadku zgodności 1, a w przypadku niezgodności -1. Iloczyn skalarny $w_i \cdot w_j$ jest zerem, co daje wynik.

(2) W tym przypadku $d_H(s_i, s_j) = n$.

(3) Stosujemy rozumowanie przypadku (1): $w_i \cdot v_j = -(w_i \cdot w_j) = 0$. Stąd $d_H(w_i, v_j) = n/2 = d_h(s_i, s_j)$.

Lemat 10.4 z rozdz. 7 o produkcie Kroneckera macierzy Hadamarda pozwala konstruować kody długości 2^n (na przykład przez „potęgowanie" macierzy $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$). Skonstruujmy dla przykładu kod (o słowach długości 8) generowany przez macierz Hadamarda podaną jako przykład w § 10, rozdz. 7. Niech H będzie następującą macierzą

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

Kod złożony z 16 słów otrzymany z macierzy H ma postać

$$\begin{array}{ll} \langle 1, 1, 1, 1, 1, 1, 1, 1\rangle, & \langle 0, 0, 0, 0, 0, 0, 0, 0\rangle, \\ \langle 1, 1, 0, 0, 1, 1, 0, 0\rangle, & \langle 0, 0, 1, 1, 0, 0, 1, 1\rangle, \\ \langle 1, 0, 1, 0, 1, 0, 1, 0\rangle, & \langle 0, 1, 0, 1, 0, 1, 0, 1\rangle, \\ \langle 1, 0, 0, 1, 1, 0, 0, 1\rangle, & \langle 0, 1, 1, 0, 0, 1, 1, 0\rangle, \end{array}$$

$$\langle 1, 1, 1, 1, 0, 0, 0, 0\rangle, \quad \langle 0, 0, 0, 0, 1, 1, 1, 1\rangle,$$
$$\langle 1, 1, 0, 0, 0, 0, 1, 1\rangle, \quad \langle 0, 0, 1, 1, 1, 1, 0, 0\rangle,$$
$$\langle 1, 0, 1, 0, 0, 1, 0, 1\rangle, \quad \langle 0, 1, 0, 1, 1, 0, 1, 0\rangle,$$
$$\langle 1, 0, 0, 1, 0, 1, 1, 0\rangle, \quad \langle 0, 1, 1, 0, 1, 0, 0, 1\rangle.$$

§ 5. Wykorzystanie konfiguracji do konstrukcji kodów

Niech $\langle X, \mathscr{B}\rangle$, $\mathscr{B} = (B_1, \ldots, B_b)$, będzie konfiguracją kwadratową o parametrach v, k, λ (por. rozdz. 7). Oznacza to, że $|X| = v$, $|B_j| = k$ dla $1 \leqslant j \leqslant b$, każda para $\{x, y\}$ należy dokładnie do λ spośród bloków $B_1, \ldots, B_b$. Rozpatrzmy macierz incydencji naszej rodziny $\mathscr{B}$. Wiersze tej macierzy są funkcjami charakterystycznymi bloków $B_1, \ldots, B_b$, kolumny zaś mówią nam, do jakich spośród zbiorów $B_1, \ldots, B_b$ należą elementy zbioru X. Badając odległość Hamminga wierszy naszej macierzy stwierdzamy, że każdy wiersz liczy dokładnie k jedynek, b zaś jest równe $\lambda\binom{v}{2}/\binom{k}{2}$ (por. (1.4), rozdział 7). Część wspólna dwóch bloków liczy λ elementów (por. tw. 2.1, rozdział 7). Informacja ta pozwala nam policzyć odległość Hamminga wierszy naszej macierzy. Mamy mianowicie $k-\lambda$ pozycji w pierwszym wierszu, gdzie pierwszy wiersz przyjmuje wartość 0, drugi zaś 1, i $k-\lambda$ pozycji o powyższej własności w drugim wierszu. Otrzymujemy stąd

TWIERDZENIE 5.1. *Jeśli $\langle X, \mathscr{B}\rangle$ jest konfiguracją kwadratową o parametrach v, k, λ, to odległość Hamminga wierszy macierzy incydencji rodziny $\mathscr{B}$ wynosi $2(k-\lambda)$, a zatem użycie wierszy tej macierzy jako słów kodowych określa kod korygujący $(k-\lambda)-1$ błędów i wykrywający $2(k-\lambda)-1$ błędów.*

Konfiguracje kwadratowe o $\lambda = 1$ są (twierdzenie 2.3, rozdział 7) dokładnie skończonymi płaszczyznami rzutowymi. W takiej sytuacji $v = n^2+n+1$, $k = n+1$, $\lambda = 1$ (pamiętamy, że znane są tylko płaszczyzny, dla których n jest potęgą liczby pierwszej). Rozważmy płaszczyznę rzutową rzędu 7 (przykład (a), § 1, rozdział 7), której macierz incydencji jest następująca:

$$A = \begin{bmatrix} 1&0&0&0&1&0&1\\ 1&1&0&0&0&1&0\\ 0&1&1&0&0&0&1\\ 1&0&1&1&0&0&0\\ 0&1&0&1&1&0&0\\ 0&0&1&0&1&1&0\\ 0&0&0&1&0&1&1 \end{bmatrix}.$$

Liczba słów kodowych wynosi 7. Możemy jednak zwiększyć liczbę takich słów dodając funkcje charakterystyczne uzupełnień naszych wierszy. Rodzina $\{X-B_1, \ldots, X-B_b\}$ jest też konfiguracją o parametrach $(v, v-k, v-2k+\lambda)$. W naszym przypadku jej macierz incydencji wygląda jak następuje:

$$\bar{A} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Zgodnie z powyższymi uwagami wiersze macierzy A (jako słowa kodujące) wykrywają 3 a korygują 1 błąd (podobnie jak uprzednio). Zbadajmy jeszcze jak różnią się między sobą wiersze macierzy A i $\bar{A}$. Otóż i-ty wiersz macierzy A różni się od j-tego wiersza macierzy $\bar{A}$ dokładnie w tych pozycjach, w którym i-ty wiersz macierzy A zgadza się z j-tym wierszem macierzy A. Tak jest w $v-2(v-k)$ pozycjach, a więc w naszym przypadku w 3 pozycjach. Zatem kod powstały z sumy A i $\bar{A}$ nadal koryguje jeden błąd (wykrywając 2 błędy). Dodajmy teraz do powstałej macierzy wiersze złożone z samych zer i jedynek. Łatwo widać, że i to rozszerzenie nie zmieni zdolności korekcyjnej naszego kodu. Otrzymujemy zatem kod o 16 słowach kodujących:

$$\begin{matrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{matrix}$$

Kod nasz wykrywa 1 błąd. Dodanie dodatkowej kolumny złożonej z 8 kolejnych jedynek i następnie 8 zer daje kod wykrywający 3 błędy i korygujący 1 błąd.

Zauważmy jeszcze, że skonstruowany przez nas kod jest doskonały (bo kula o promieniu 1 liczy w naszym wypadku $1+7 = 8 = 2^3$ elementów, słów kodujących jest 2^4, wszystkich zaś słów jest $2^7 = 2^4 \cdot 2^3$). Nic dziwnego, jest to bowiem (7, 4)-kod Hamminga.

§ 6. Kod Golay'a

Jak łatwo stwierdzić, liczba 23 ma następującą własność

$$\binom{23}{0}+\binom{23}{1}+\binom{23}{2}+\binom{23}{3} = 2048 = 2^{11}.$$

Skoro przestrzeń $(GF(2))^{23}$ liczy 2^{23} wektorów, a kula $S_3(x)$ liczy w tej przestrzeni właśnie tyle, ile wynosi lewa strona naszej równości, a więc 2^{11} wektorów, przeto – *a priori* – jest szansa na to, że istnieje kod doskonały, o słowach długości 23 (z 12 symbolami informacyjnymi – słów kodowych byłoby bowiem 2^{12}). Jest tak w istocie: poniżej skonstruujemy (23, 12)-kod liniowy korygujący 3 błędy. Kod ten jest zatem kodem doskonałym, ponieważ $S_3(x) = 2^{11}$, zaś $2^{11}2^{12} = 2^{23}$.

W tym celu zauważmy, że $2^{11}-1 = 23 \cdot 89$, a zatem $GF(2^{11})$ zawiera element pierwotny rzędu 23. Rozważmy taki element a i jego wielomian minimalny, który (por. dowód twierdzenia 31, Dodatek) ma postać $\prod_{i=0}^{10}(x-a^{2^i})$. Stwierdzamy natychmiast, że $a^{32} = a^9$, $a^{64} = a^{18}$, $a^{128} = a^{13}$, $a^{256} = a^3$, $a^{512} = a^6$, $a^{1024} = a^{12}$ (bowiem $32 \equiv 9 \pmod{23}$ itd.). Wielomian nasz ma zatem postać

$$g(x) = \prod_{i\in A}(x-a^i), \qquad \text{gdzie } A = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}.$$

Dla elementu $a^{-1} = a^{22}$ wielomian minimalny ma postać

$$\prod_{i=0}^{10}(x-a^{22\cdot 2^i}),$$

co daje

$$h(x) = \prod_{i\in B}(x-a^i), \qquad \text{gdzie } B = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}.$$

Stwierdzamy, że $A \cap B = 0$, $A \cup B = \{1, \ldots, 22\}$, a zatem każdy element rzędu 23 (poza jedynką) jest pierwiastkiem albo $g(x)$, albo $h(x)$. Stąd $x^{23}-1 = (x-1)\,g(x)\,h(x)$.

Definiujemy teraz *kod Golay'a K* jako zbiór ciągów $\langle a_0, \ldots, a_{22}\rangle$ takich, że $g(x) \mid \sum_{j=0}^{22} a_j x^j$.

Już z samej definicji wynika natychmiast, że zdefiniowany kod jest kodem liniowym. Dalej, każde słowo kodu jest wyznaczone przez wielomian $I(x)$ taki, że $\deg I \leqslant 11$. Odwrotnie, każdy wielomian stopnia co najwyżej 11 wyznacza słowo kodowe. Kod nasz ma zatem wymiar 12. Dla wykazania, że jest on kodem doskonałym korygującym 3 błędy, wykażemy, że $d_H(\mathbf{x}, \mathbf{y}) \geqslant 7$ dla $\mathbf{x}, \mathbf{y} \in K$, $\mathbf{x} \neq \mathbf{y}$. Ponieważ kod nasz jest liniowy, wystarczy wykazać, że waga minimalna elementów kodu jest co najmniej równa 7.

LEMAT 6.1. *Waga każdego słowa kodu K jest równa co najmniej 5.*

Dowód. Utożsamiajmy słowo kodowe $\mathbf{x}$ z wielomianem zgodnie z powyższą metodą: $\mathbf{x}(a) = \mathbf{x}(a^2) = \mathbf{x}(a^3) = \mathbf{x}(a^4) = 0$ zgodnie z postacią wielomianu g. Stąd ciąg $\mathbf{x}$ spełnia równość

$$\mathbf{x} \cdot H^T = 0,$$

gdzie H jest równe

$$\begin{bmatrix} 1 & a & a^2 \dots a^{22} \\ 1 & a^2 & a^4 \dots a^{44} \\ 1 & a^3 & a^6 \dots a^{66} \\ 1 & a^4 & a^8 \dots a^{88} \end{bmatrix}.$$

Jeśli słowo kodowe ma wagę $\leqslant 4$, to stosując ten sam pomysł co w dowodzie twierdzenia 3.1 (badanie wyznacznika Vandermonde'a) stwierdzamy, że musi ono być zerem. To dowodzi lematu. □

Ponieważ słowo $\mathbf{1} = \langle 1, \dots, 1 \rangle$ należy do kodu K (gdyż $y(x) \cdot h(x) = \mathbf{1}$), zatem ilekroć słowo $\mathbf{x}$ o wadze i należy do K, to także słowo $\mathbf{1} - \mathbf{x}$ należy do K. Oznaczając przez A_j liczbę słów w K o wadze j, mamy $A_j = A_{23-j}$. Dla wykazania głównego rezultatu naszego paragrafu musimy dowieść, że $A_5 = 0 = A_6$ (dla wykazania pierwszej z tych równości wystarczy dowieść, że $A_{18} = 0$).

TWIERDZENIE 6.2. *Jeśli $\mathbf{y}$ jest słowem kodowym o wadze parzystej, to* $4|w(\mathbf{y})$.

Dowód. Rozważmy $\mathbf{y}(x)$. Skoro $\mathbf{y} \in K$, mamy $g(x)|\mathbf{y}(x)$, przy czym $\mathbf{y}$ ma wagę parzystą, co oznacza, że $y(1) = 0$, czyli $(x-1)|\, y(x)$. Niech $y(x) = x^{a_1} + x^{a_2} + \dots$ $\dots + x^{a_r}$, $0 \leqslant a_1 < \dots < a_r \leqslant 22$. Określmy $z(x) = x^{-a_1} + x^{-a_2} + \dots + x^{-a_r}$ $(-a_1, \dots, -a_r$ obliczamy modulo 23). Wówczas $z(a^{-1}) = 0$, co zgodnie z własnościami wielomianu $h(x)$ oznacza, że $h(x)|z(x)$. Stąd

$$(x-1)\, g(x) h(x) | \mathbf{y}(x)\, z(x),$$

czyli

$$(x^{23} - 1) | \mathbf{y}(x)\, z(x).$$

Policzymy teraz $\mathbf{y}(x)\, z(x) \pmod{x^{23} - 1}$:

$$\mathbf{y}(x)\, z(x) = \sum_{j=1}^{r} x^{a_j} \sum_{j=1}^{r} x^{-a_j} = \sum_{i,j=1}^{r} x^{a_i - a_j}.$$

Zatem $y(x)z(x) (\mathrm{mod}\, x^{23}-1)$ jest równe

$$r+\Big(\sum_{\substack{i,j=1\\ i\neq j}}^{r} x^{a_i-a_j}\Big) (\mathrm{mod}\, x^{23}-1).$$

Z założenia r jest parzyste, zatem jest zerem w $GF(2)$. Stąd $y(x)z(x) \equiv \equiv \sum_{k=0}^{22} c_k x^k (\mathrm{mod}\, x^{23}-1)$, gdzie c_k jest liczbą par $\langle i, j\rangle$ takich, że $a_i - a_j \equiv k (\mathrm{mod}\, 23)$. Ponieważ $(x^{23}-1) | y(x)z(x)$, więc każde c_k jest parzyste. Z faktu, że $a_i - a_j \equiv k (\mathrm{mod}\, 23)$ wynika, iż $a_j - a_i \equiv 23-k (\mathrm{mod}\, 23)$, zatem

(6.1) $$c_k = c_{23-k}.$$

Zauważmy, że iloczyn $y(x)z(x)$ ma r^2-r wyrazów nie będących liczbami. Stąd

$$\sum_{k=1}^{22} c_j = r^2-r.$$

Ze względu na równość (6.1) mamy

$$2\sum_{k=1}^{11} c_k = r^2-r = r(r-1).$$

Każde c_k było parzyste, zatem lewa strona jest podzielna przez 4, a ponieważ r było parzyste, więc $4|r$. □

Sumując informację uzyskaną w lemacie 6.1 i twierdzeniu 6.2 wraz z uwagami poprzedzającymi twierdzenie 6.2 otrzymujemy

TWIERDZENIE 6.3. *Kod Golay'a jest doskonałym* (23, 12)-*kodem liniowym.* □

Niestety, konstrukcja Golay'a nie uogólnia się. Poza kodami Hamminga i kodem Golay'a znany jest tylko jeden kod doskonały; jest to (11, 6)-kod nad $GF(3)$. Jest to kod korygujący 2 błędy. Konstrukcja tego kodu, którą zostawiamy Czytelnikowi, jest podobna do powyższej konstrukcji (por. zadania).

§ 7. Numerator kodu, twierdzenie MacWilliams

Niech $C \subseteq (GF(q))^n$ będzie kodem liniowym. Zbiór C rozpada się w naturalny sposób na sumę $C = \bigcup_{j=0}^{n} C_j$, gdzie C_j składa się ze słów kodowych o wadze równej j. Niech $A_j = |C_j|$, $0 \leqslant j \leqslant n$.

Numeratorem kodu C nazywamy wielomian $W_C(x, y)$ dwóch zmiennych x i y określony jak następuje:

$$W_C(x, y) = \sum_{j=0}^{n} A_j x^{n-j} y^j.$$

Zauważmy, że $W_C(x, y)$ jest jednorodny, tj. $W_C(\alpha x, \alpha y) = \alpha^n W_C(x, y)$. Oznaczając przez $w(\boldsymbol{u})$ wagę słowa $\boldsymbol{u}$ mamy

$$W_C(x, y) = \sum_{\boldsymbol{u} \in C} x^{n - w(\boldsymbol{u})} \cdot y^{w(\boldsymbol{u})}.$$

Podajmy przykłady numeratorów konkretnych kodów. Kod $\{\langle 00\rangle, \langle 11\rangle\}$ (a więc powtarzający słowa kodowane długości 1 — mianowicie 0 i 1 — dwukrotnie) ma numerator równy x^2+y^2. Kod $\{\langle 0, 0, 0\rangle, \langle 1, 0, 0\rangle, \langle 0, 1, 0\rangle, \langle 1, 1, 0\rangle\}$ ma następujący numerator: $x^3+2x^2y+xy^2$.

Kod Hamminga (skonstruowany przez nas (7, 4)-kod doskonały) ma numerator $x^7+7x^4y^3+7x^3y^4+y^7$. Dla dowodu wystarczy zauważyć, że kod Hamminga został skonstruowany przez nas z płaszczyzny Fano (por. rozdz. 7, § 11) w ten sposób, że oprócz wierszy macierzy incydencji płaszczyzny Fano (7 wierszy — każdy o wadze 3) wzięliśmy ich uzupełnienia (7 wierszy — każdy o wadze 4) i dodaliśmy słowa $\langle 0, \ldots, 0\rangle$ i $\langle 1, \ldots, 1\rangle$.

Rozszerzony kod Hamminga (poprzez dodanie kontroli parzystości) ma numerator następujący: $x^8+14x^4y^4+y^8$. Łatwo na tej podstawie opracować ogólne przejście z numeratorów kodów do numeratorów kodów rozszerzonych o kontrolę parzystości.

Zasadniczym wynikiem dotyczącym numeratorów kodów jest twierdzenie MacWilliams, które orzeka, że numerator kodu dualnego do kodu C jest wyznaczony w sposób konstruktywny przez numerator kodu C. Do dowodu tego twierdzenia będziemy potrzebowali skromnego aparatu teorii reprezentacji grup. *Charakterem grupy* $\langle A, +\rangle$ nazywamy homomorfizm grupy $\langle A, +\rangle$ w grupę $\langle \mathbf{C}-\{0\}, \cdot\rangle$.

Następujących faktów dotyczących charakterów Czytelnik dowiedzie łatwo sam lub znajdzie w podręczniku teorii grup (p. też Dodatek).

LEMAT 7.1. *Jeśli φ jest nietrywialnym charakterem grupy skończonej $\langle A, +\rangle$ (tj. dla pewnego $x \neq 0$, $\varphi(x) \neq 1$), to*

(a) *Dla każdego x jest $|\varphi(x)| = 1$,*

(b) $\sum_{x \in A} \varphi(x) = 0$.

Pierwszy z tych faktów wynika stąd, że $x^{|A|} = 1$ dla dowolnego $x \in A$, drugi stąd, że mnożenie przez element jest automorfizmem wewnętrznym. □

LEMAT 7.2. *Niech φ będzie nietrywialnym charakterem grupy $\langle GF(q), +\rangle$ i dla $\boldsymbol{v} \in (GF(q))^n$ określmy*

$$\varphi_{\boldsymbol{v}}(\boldsymbol{u}) = \varphi((\boldsymbol{u}, \boldsymbol{v})),$$

gdzie $\boldsymbol{u} \cdot \boldsymbol{v}$ jest iloczynem skalarnym w $(GF(q))^n$. Dla dowolnego f: $(GF(q))^n \to A$, gdzie A jest przestrzenią liniową nad $\mathbf{C}$, zdefiniujmy

$$\hat{f}(\boldsymbol{u}) = \sum_{\boldsymbol{v} \in (GF(q))^n} f(\boldsymbol{v}) \cdot \varphi_{\boldsymbol{v}}(\boldsymbol{u}).$$

Wówczas dla dowolnej podprzestrzeni liniowej $C \subseteq (GF(q))^n$

$$\sum_{u \in C} \hat{f}(u) = |C| \sum_{v \in C^{\perp}} f(v).$$

Dowód.

$$\sum_{u \in C} \hat{f}(u) = \sum_{u \in C} \sum_{v \in (GF(q))^n} f(v) \cdot \varphi_v(u) =$$
$$= \sum_{v \in (GF(q))^n} f(v) \cdot \sum_{u \in C} \varphi(u \cdot v) =$$
$$= \sum_{v \in C^{\perp}} f(v) \sum_{u \in C} \varphi(u \cdot v) + \sum_{v \notin C^{\perp}} f(v) \sum_{u \in C} \varphi(u \cdot v).$$

W pierwszej z sum mamy $v \in C^{\perp} \wedge u \in C \Rightarrow u \cdot v = 0$. Zatem $\varphi(u \cdot v) = 1$ a suma wewnętrzna jest równa $|C|$. Stąd pierwszy człon jest równy $|C| \sum_{v \in C^{\perp}} f(v)$. Wykażemy, że druga suma jest zerem. W tym celu udowodnimy, że dla $v \notin C^{\perp}$, $\sum_{u \in C} \varphi(u \cdot v) = 0$.

Najpierw zauważmy, że jeśli $v \notin C^{\perp}$, to $u \cdot v$ dla $u \in C$ przyjmuje każdą wartość taką samą liczbę razy. Istotnie, niech $a_1, \ldots, a_k$ będą wartościami, a $C = C_{a_1} \cup \ldots \cup C_{a_k}$ rozkładem C na sumę przeciwobrazów.

Możemy założyć, że $a_1 = 0$ (gdyż $0, v = 0$); wybierając $u_2, \ldots, u_k$ z $C_{a_2}, \ldots, C_{a_k}$ mamy

$$w \in C_0 \Leftrightarrow w + u_j \in C_{a_j}.$$

To dowodzi, że $|C_0| = |C_{a_1}| = \ldots = |C_{a_k}|$, czyli że wartość ta przyjmowana jest taką samą liczbę razy.

Wystarczy teraz wykazać, że $\{u \cdot v \colon u \in C\}$ (pamiętamy, że $v \notin C^{\perp}$) jest całym ciałem $GF(q)$. Istotnie, dla choć jednego $u \in C$, $u \cdot v \neq 0$. Niech $u \cdot v = a \neq 0$ i niech $b \in GF(q)$; wówczas $a^{-1} bu \cdot v = b$.

Jeśli zatem $k = |C_0|$, to

$$\sum_{u \in C} \varphi(u \cdot v) = k \sum_{a \in GF(q)} \varphi(a) = k \cdot 0 = 0,$$

jeśli bowiem φ jest charakterem nietrywialnym, to

$$\sum_{a \in GF(q)} \varphi(a) = 0. \quad \square$$

Zauważmy na marginesie tego dowodu, że ponieważ rząd addytywny każdego elementu z $GF(p^n)$ jest równy p, więc wartości charakteru mają multyplikatywny rząd równy p, a zatem są pierwiastkami p-tego stopnia z jedności. Stąd, jeśli charakter φ jest nietrywialny, to $\{\varphi(a) \colon a \in GF(p^n)\}$ składa się dokładnie z pierwiastków p-tego stopnia z jedności.

Korzystając z powyższego lematu wykażemy

TWIERDZENIE 7.3. *Jeśli $W_C(x, y)$ jest numeratorem (n, k)-kodu liniowego C, to $q^{-k}W(x+(q-1)y,\ x-y)$ jest numeratorem kodu dualnego $C^{\perp}$.*

Dowód. Skorzystamy z lematu 7.2 w następującej sytuacji. A jest przestrzenią wielomianów dwóch zmiennych nad ciałem liczb zespolonych, $f(v) = x^{n-w(v)}y^{w(v)}$, dla $a \in GF(q)$ zaś przyjmujemy $w(a)$ równe jedności, jeśli $a \neq 0$, $w(0) = 0$. Niech wreszcie φ będzie dowolnym różnowartościowym charakterem na $\langle GF(q), +\rangle$ (np. reprezentacja $\langle GF(q), +\rangle$ za pomocą pierwiastków stopnia q z jedności). Rozważmy

$$\hat{f}(u) = \sum_{v\in(GF(q))^n} f(v)\cdot\varphi_v(u) = \tag{7.1}$$

$$= \sum_{v\in(GF(q))^n} x^{n-w(v)}\, y^{w(v)}\, \varphi(u\cdot v),$$

ponieważ

$$n-w(v) = \sum_{i=1}^{n} (1-w(v_i)),$$

$$w(v) = \sum_{i=1}^{n} w(v_i),$$

$$\varphi(u\cdot v) = \prod_{i=1}^{n} \varphi(u_i v_i).$$

(Ostatnia równość wynika stąd, że φ jest charakterem.) Możemy zatem sumę (7.1) przedstawić jako

$$\sum_{v_1\in GF(q)} \cdots \sum_{v_n\in GF(q)} x^{1-w(v_1)+\ldots+1-w(v_n)}\, y^{w(v_1)+\ldots+w(v_n)} \prod_{i=1}^{n} \varphi(u_i v_i) =$$

$$= \prod_{i=1}^{n} \sum_{v\in GF(q)} x^{1-w(v)} y^{w(v)}\, \varphi(u_i v).$$

Zbadajmy sumę po znaku iloczynu. Jest ona równa

$$x+(q-1)y \quad \text{dla } u_i = 0 \quad (\text{gdyż wtedy } \varphi(u_i v) = \varphi(0) = 1),$$

natomiast dla $u_i \neq 0$ mamy składnik x dla $v = 0$ i jeszcze sumę

$$\sum_{v\in GF(q)\setminus\{0\}} y^{w(v)}\, \varphi(u_i v);$$

jest ona równa $y \underset{v\in GF(q)\setminus\{0\}}{M} \varphi(u_j v) = -y$, gdyż $u_j \neq 0$ implikuje, że $\{u_j v\colon v\in GF(q)\setminus\{0\}\} = GF(q)\setminus\{0\}$, przy czym $\sum_{v\in GF(q)} \varphi(v) = 0$, zaś $\varphi(0) = 1$. Stąd $\hat{f}(u) = (x+(q-1)y)^{n-w(u)}(x-y)^{w(u)}$.

Teraz już — po „pozbyciu się" charakteru φ i szczegółowym przedstawieniu $\hat{f}$ w zależności od f — zastosujmy lemat 7.2. Mamy:

$$W_{C^\perp}(x, y) = \sum_{v\in C^\perp} x^{n-w(v)}y^{w(v)} = \sum_{v\in C^\perp} f(v) = \frac{1}{|C|}\sum_{u\in C}\hat{f}(u) = \frac{1}{q^k}W_C\big(x+(q-1)y,\ x-y\big),$$

co kończy dowód. □

W przypadku binarnym mamy

Wniosek 7.4. $W_{C^\perp}(x, y) = \frac{1}{2^k}W_C(x+y,\ x-y)$.

Jeśli kod C jest dualny, tj. $C = C^\perp$, to k musi być równe $n/2$, wtedy $W_C = W_{C^\perp} = W_C\left(\frac{x+y}{\sqrt{2}}, \frac{x-y}{\sqrt{2}}\right)$ (na mocy jednorodności), to zaś natychmiast wiąże naszą teorię z teorią inwariantów, bardzo głębokim działem algebry. Nie będziemy tutaj wskazywali na zastosowania tej teorii do teorii kodów, wspomnijmy tylko, że N. J. A. Sloane [1] daje przegląd takich możliwości.

§ 8. Kody Reeda–Mullera

Będziemy rozważali klasę kodów, która jest naturalnym uogólnieniem rozszerzonego kodu Hamminga, tj. kodu powstającego z kodu Hamminga poprzez dodanie kontroli parzystości. Wprowadźmy w przestrzeni liniowej $(GF(2))^k$ działanie mnożenia wzorem:

$$\boldsymbol{ab} = \boldsymbol{c} \Leftrightarrow a_j\cdot b_j = c_j,\ 1 \leqslant j \leqslant k.$$

Mamy oczywiście $\boldsymbol{a}\boldsymbol{a} = \boldsymbol{a}$.

Rozważmy teraz macierz o wymiarze $n\times 2^n$, której kolumnami są kolejno rozwinięcia dwójkowe liczb naturalnych $0, \ldots, 2^n-1$ z tym, że pisane „z góry na dół". Dla $n = 4$ macierz ta ma postać:

$$\begin{bmatrix} 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1 \end{bmatrix}$$

Nazwijmy wiersze tej macierzy kolejno $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$ (w naszym przypadku $n = 4$). Nazwijmy $\boldsymbol{v}_0$ wiersz złożony z samych jedynek. Ponieważ kolumny naszej macierzy są wszystkimi wektorami przestrzeni $(GF(2))^n$, spróbujmy dać „mnogościową" interpretację wektorów $\boldsymbol{v}_j$ $(0 \leqslant j \leqslant n)$. Niech zatem wektory z $(GF(2))^n$ będą ponumerowane liczbami $0, \ldots, 2^n-1$. Wtedy $\boldsymbol{v}_j$ jest funkcją charakterystyczną zbioru tych spośród wektorów, które na j-tej współrzędnej mają 1 ($\boldsymbol{v}_0$ jest funkcją

charakterystyczną całej przestrzeni). Łatwo widać, że dla $i \neq j$, $v_i v_j$ jest funkcją charakterystyczną zbioru tych wektorów z $(GF(2))^n$, które mają jedynki zarówno na i-tej jak i na j-ej współrzędnej.

Uogólniając to rozumowanie stwierdzamy, że $v_{i_1} v_{i_2} \ldots v_{i_k}$ jest funkcją charakterystyczną zbioru tych wektorów z $(GF(2))^n$ które mają jedynki na współrzędnych $i_1, i_2, \ldots, i_k$. Ponieważ na współrzędnych różnych od $i_1, \ldots, i_k$ są możliwe obie wartości, zero i jeden, więc $v_{i_1} \ldots v_{i_k}$ jest funkcją charakterystyczną zbioru o liczności 2^{n-k}, co oznacza w naszym przypadku, że waga $w(v_{i_1} \ldots v_{i_k})$ jest równa 2^{n-k}.

Rozważmy teraz wszystkie możliwe iloczyny $v_0 v_{i_1} \ldots v_{i_k}$, gdzie $1 \leqslant i_1 < i_2 < \ldots < i_k \leqslant n$ (zauważmy, że $v_0 a = a$, a zatem możemy v_0 w iloczynie opuszczać).

TWIERDZENIE 8.1. *Wektory* $v_0, v_{i_1}, \ldots, v_{i_k}$ *tworzą bazę przestrzeni* $(GF(2))^{2^n}$.

Dowód. Rodzina naszych wektorów liczy

$$1 + \sum_{j=1}^{n} \binom{n}{j} = 2^n$$

wektorów. Wystarczy zatem wykazać, że rozpinają one całą przestrzeń $(GF(2)^2)^n$, czyli że wszystkie wektory $e_j = \langle 0, \ldots, 0, 1, 0, \ldots, 0 \rangle$ (jedna jedynka na j-ej współrzędnej) są kombinacjami liniowymi wektorów z naszej rodziny. W tym celu niech liczba j ma rozwinięcie $\langle a_1, \ldots, a_n \rangle$. Ilekroć $a_k = 0$, niech $S_k = v_k + v_0$, ilekroć zaś $a_k = 1$, niech $S_k = v_k$. Rozważmy iloczyn $S_1 \ldots S_n$. Ponieważ każdy z wektorów S_k ma na j-ej współrzędnej 1, przeto iloczyn nasz ma na j-ej współrzędnej 1. Jednakże $v_k + v_0$ jest funkcją charakterystyczną zbioru będącego uzupełnieniem zbioru, którego funkcją charakterystyczną jest v_k, tj. zbioru tych liczb, które na k-tej współrzędnej mają 0.

Iloczyn wektorów jest funkcją charakterystyczną iloczynu mnogościowego, stąd iloczyn $S_1 \ldots S_n$ jest funkcją charakterystyczną zbioru wektorów (z $(GF(2))^n$), które na pierwszej współrzędnej mają a_1, na drugiej a_2 itd. Ale taki wektor jest tylko jeden. Stąd $S_1 \ldots S_n$ ma wagę równą 1, a ponieważ na j-ej współrzędnej ma 1, zatem jest to e_j. Zauważmy teraz, że

$$S_k = v_k + (1 + a_k) v_0 .$$

Iloczyn $S_1 \ldots S_n$ ma zatem postać $\prod_{k=1}^{n} (v_k + (1 + a_k) v_0)$, a ponieważ nasze mnożenie jest rozdzielne względem dodawania, e_j jest sumą pewnych spośród wektorów v_0, $v_{i_1} \ldots v_{i_k}$, co było do wykazania. □

Kodem Reeda–Mullera rzędu r długości 2^n nazywamy podprzestrzeń przestrzeni $(GF(2))^n$, której bazę tworzą wektory v_0 oraz wszystkie iloczyny $v_{i_1} \ldots v_{i_k}$ dla $k \leqslant r$. Jako przykład rozważmy kod Reeda–Mullera rzędu 2 i długości 16. Ma on macierz generującą:

$$\begin{bmatrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 0&1&0&1&0&1&0&1&0&1&0&1&0&1&0&1\\ 0&0&1&1&0&0&1&1&0&0&1&1&0&0&1&1\\ 0&0&0&0&1&1&1&1&0&0&0&0&1&1&1&1\\ 0&0&0&0&0&0&0&0&1&1&1&1&1&1&1&1\\ 0&0&0&1&0&0&0&1&0&0&0&1&0&0&0&1\\ 0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&1\\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&0&1\\ 0&0&0&0&0&0&1&1&0&0&0&0&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&1&1&0&0&1&1\\ 0&0&0&0&0&0&0&0&0&0&0&0&1&1&1&1 \end{bmatrix}.$$

Kod ten ma wymiar 11.

TWIERDZENIE 8.2. *Kodem ortogonalnym do kodu Reeda–Mullera rzędu k i długości 2^n jest kod Reeda–Mullera rzędu $n-k-1$ tej samej długości.*

Dowód. Zauważmy, że wektory $v_{i_1}\dots v_{i_r}$, $v_{j_1}\dots v_{j_i}$ są ortogonalne. Istotnie, iloczyn skalarny $u\cdot v$ jest równy sumie współrzędnych iloczynu $u\cdot v$. Jednakże, jeśli iloczyn jest przemienny i łączny, przy czym $a^2=a$, to iloczyn $v_{i_1}\dots v_{i_r}v_{j_1}\dots v_{j_i}$ jest też wektorem postaci $v_{s_1}\dots v_{s_t}$. Jednakże waga takiego wektora jest równa 2^{n-t}, co oznacza że suma współrzędnych tego wektora jest zerem. Teraz zauważmy, że wymiar kodu Reeda–Mullera rzędu k (długości 2^n) wynosi $1+\binom{n}{1}+\dots+\binom{n}{k}$, dla takiego zaś kodu rzędu $n-k-1$ wynosi $1+\binom{n}{1}+\dots$ $\dots+\binom{n}{n-k-1}=\binom{n}{n}+\binom{n}{n-1}+\dots+\binom{n}{k+1}$.

Ponieważ suma wymiarów wynosi 2^n (zgodnie z tożsamością $\sum_{j=0}^{n}\binom{n}{j}=2^n$), nasze twierdzenie zostało wykazane. □

Wynika stąd też bezpośrednio, że kod Reeda–Mullera rzędu $n-2$ jest rozszerzonym $(2^n,\ 2^n-n-1)$-kodem Hamminga.

Dla zbadania możliwości kodowania i odkodowywania przy użyciu kodów Reeda–Mullera musimy wiedzieć więcej na temat sposobu, w jaki wektory przestrzeni $(GF(2))^{2^n}$ rozwijają się w zdefiniowanej powyżej bazie.

Niech $1\leqslant i_1<\dots<i_k\leqslant n$. Dla $0\leqslant j\leqslant 2^{n-1}$, j ma jedyną reprezentację $j=\sum_{i=1}^{n}a_{ij}2^{i-1}$. Niech $A_j=\{i\colon a_{ij}=0\}$, zaś $B_j=\{1,\dots,n\}-A_j=\{i\colon a_{ij}=1\}$. Określamy teraz $C(i_1,\dots,i_k)=\{j\colon \{i_1,\dots,i_k\}\subseteq B_j\}$. Stąd $C(i_1,\dots,i_k)$ jest zbiorem tych liczb, których rozwinięcia dwójkowe mają jedynki na pozycjach co najwyżej $i_1,\dots,i_k$, poza tymi zaś pozycjami — na pewno zero.

Korzystając z powyższej definicji wykażemy, w jaki sposób zmieniamy rozwinięcie w bazie $\langle e_j \rangle_{j=0}^{2^n-1}$ na rozwinięcie w bazie $v_0 v_{i_1} \ldots v_{i_k}$, $0 \leqslant i_1 < \ldots$ $\ldots < i_k \leqslant 2^n - 1$.

Niech zatem $a = \sum_{j=0}^{m-1} a_j e_j$ $(m = 2^n)$. Jak pamiętamy, $e_j = \prod_{i=1}^{n} s_i$, $s_i = v_i + (1 + a_{ij}) v_0$. Tak więc w iloczynie naszym występuje v_i, jeśli $a_{ij} = 0$, i $v_i + v_0$, jeśli $a_{ij} = 1$. Teraz możemy już znaleźć warunek, przy którym iloczyn $v_{i_1} \ldots v_{i_k}$ będzie występował w rozwinięciu e_j. Musimy mianowicie w trakcie wymnażania mieć możliwość brania v_0 na każdej pozycji nie należącej do $\{i_1, \ldots, i_k\}$. Oznacza to, że jeśli $j \notin \{i_1, \ldots, i_k\}$, to $a_{ij} = 0$, tj. jeśli $a_{ij} = 1$, to $j \in \{i_1, \ldots, i_k\}$, czyli $\{i_1, \ldots, i_k\} \subseteq B_j$, tj. $j \in C(i_1, \ldots, i_k)$. Oczywiście jest to warunek konieczny i dostateczny.

Tak więc

$$e_j = \sum_{k=0}^{n} \{v_{i_1} \ldots v_{i_k} \colon 1 \leqslant i_1 < \ldots < i_k \wedge j \in C(i_1, \ldots, i_k)\}.$$

Teraz już mamy natychmiast:

$$a = \sum_{j=0}^{m-1} a_j e_j = \sum_{j=0}^{m-1} a_j \sum_{k=0}^{n-1} \{v_{i_1} \ldots v_{i_k} \colon i_1 < \ldots < i_k \wedge j \in C(i_1, \ldots, i_k)\};$$

zmieniając porządek sumowania otrzymujemy

$$a = \sum_{k=0}^{n-1} \sum_{i_1 < \ldots < i_k} \Big(\sum_{j \in C(i_1, \ldots, i_k)} a_j \Big) v_{i_1} \ldots v_{i_k}. \tag{8.1}$$

Możemy teraz przystąpić do kodowania. Niech $N = \sum_{j=0}^{r} \binom{n}{j}$ i niech liczby $\langle 0, \ldots, N-1$ numerują ciągi $v_{i_1} \ldots v_{i_k}$, $i_1 < \ldots < i_k$, $k \leqslant r$.

Możemy założyć, że dłuższe iloczyny są kodowane przez większe liczby. Przyjmujemy dla słowa kodowanego długości N, $\langle a_0, \ldots, a_{N-1} \rangle$, słowo kodowe

$$c = a_0 v_0 + a_1 v_1 + \ldots + a_{N-1} v_{m-r+1} \ldots v_m.$$

Słowo kodowe ma zatem długość m, podczas gdy kodowane długość N.

Jeśli zatem nadaliśmy słowo $c = \langle c_0, \ldots, c_{m-1} \rangle$ i otrzymaliśmy je, to znalezienie słowa $\langle a_0, \ldots, a_{N-1} \rangle$ jest proste. Zgodnie z metodą zamiany rozwinięcia, jeśli c jest słowem kodowym, s zaś numerem iloczynu $v_{i_1} \ldots v_{i_r}$, to

$$a_s = \sum_{j \in C(i_1, \ldots, i_r)} c_j.$$

To oczywiście nie rozwiązuje problemu korekcji. Dla jego zbadania załóżmy, że kod nasz jest kodem Reeda–Mullera rzędu r, a zatem podprzestrzeń słów kodowych jest rozpięta przez iloczyny długości co najwyżej r. Innymi słowy żaden iloczyn długości $r+1$ w rozwinięciu słowa kodowanego nie wystąpi. Oznacza to, że

jeśli $i_1 < \ldots < i_r$, $t \notin \{i_1, \ldots, i_r\}$, $\boldsymbol{a}$ zaś jest słowem kodowym, to

$$\sum_{j \in C(i_1, \ldots, i_r, t)} a_j = 0 \tag{8.2}$$

(zgodnie z (8.1)).

Jednakże $C(i_1, \ldots, i_r, t)$ rozpada się na zbiory rozłączne tych liczb, które na pozycji t mają zero, oraz tych, które na pozycji t mają jedność. Tak więc

$$C(i_2, \ldots, i_r, t) = C(i_1, \ldots, i_r) \cup \{j + 2^{t-1}\colon j \in C(i_1, \ldots, i_r)\}.$$

Z (8.2) i faktu, że $-x = x$ znajdujemy

$$a_s = \sum_{j \in C(i_1, \ldots, i_r)} c_{j+2^{t-1}} \qquad (t \notin C(i_1, \ldots, i_r)).$$

Rozważmy teraz zbiór $C(i_1, \ldots, i_r, t_1, t_2)$. Zbiór ten rozpada się na 4 podzbiory $C(i_1, \ldots, i_r)$, $\{j + 2^{t_1-1}\colon j \in C(i_1, \ldots, i_r)\}$, $\{j + 2^{t_2-1}\colon j \in C(i_1, \ldots, i_r)\}$ oraz resztę, tj. $\{j + 2^{t_1-1} + 2^{t_2-1}\colon j \in C(i_1, \ldots, i_r)\}$. Dla każdego z trzech pierwszych zbiorów suma $\sum c_j$ była równa a_s. Skoro suma $\sum \{c_j\colon j \in C(i_1, \ldots, i_r, t_1, t_2)\}$ jest zerem, to dla czwartego z tych zbiorów odpowiednia suma wynosi również a_s. Teraz rozumujemy indukcyjnie i otrzymujemy następujące twierdzenie.

TWIERDZENIE 8.3. *Jeśli s jest numerem iloczynu $v_{i_1} \ldots v_{i_r}$, to istnieje podział zbioru $\{0, 1, \ldots, m-1\}$ na 2^{n-r} zbiorów rozłącznych, każdy liczący 2^r elementów, tak, by dla każdego zbioru Z należącego do naszej rodziny, $a_s = \sum \{c_j\colon j \in Z\}$.*

Dowód. Łatwo widać, że żądana rodzina powstaje w następujący sposób. Uzupełnienie zbioru $\{i_1, \ldots, i_r\}$ liczy $n-r$ elementów, dla każdego zbioru $T \subseteq \{1, \ldots, n\} - \{i_1, \ldots, i_r\}$ zbiór $Z_T = \{j + \sum_{t \in T} 2^{t-1}\colon j \in C(i_1, \ldots, i_r)\}$ liczy 2^r elementów (tyle ile $C(i_1, \ldots, i_r)$). Jeśli $T_1 \neq T_2$, to $Z_{T_1} \cap Z_{T_2} = \emptyset$.

Wreszcie (i tu właśnie używamy rozumowania indukcyjnego ze względu na liczbę elementów w zbiorze T) $\sum \{c_j\colon j \in Z_T\} = a_s$. Ponieważ istnieje dokładnie 2^{n-r} zbiorów T jak wyżej, twierdzenie nasze jest udowodnione. □

Możemy teraz wskazać metodę korekcji co najwyżej $2^{n-r-1}-1$ błędów. Przypuśćmy, że otrzymaliśmy słowo $\langle d_0, \ldots, d_{m-1} \rangle$, a popełniono nie więcej niż $2^{n-r-1}-1$ błędów.

Gdyby błędów nie było, to $a_s = \sum \{d_j\colon j \in Z_T\}$ dla każdego $T \subseteq \{1, \ldots, n\} - \{i_1, \ldots, i_r\}$. Ale ponieważ popełniliśmy błędy, pewna część spośród powyższych równości przestanie mieć miejsce. Zbadajmy zatem, jak wiele spośród nich zostanie naruszonych. Otóż widać, że co najmniej $2^{n-r-1}+1$ spośród zbiorów Z_T da w dalszym ciągu taką samą sumę, mianowicie a_s. Wobec tego postępujemy następująco: Jeśli większość sum odpowiadających a_s wynosi 1, to stwierdzamy, że a_s równe jest 1 i odkodowujemy a_s jako 1, w przeciwnym przypadku 0. Postępujemy tak dla każdego zbioru r-elementowego $\{i_1, \ldots, i_r\}$. Od otrzymanego słowa $\langle d_0, \ldots, d_{m-1} \rangle$ odejmujemy słowa $a_s v_{i_1} \ldots v_{i_r}$ (dla wszystkich s będących numera-

mi r-elementowych ciągów). Tak otrzymane słowo jest otrzymane ze słowa kodu Reeda–Mullera rzędu $r-1$, a zatem postępujemy podobnie (zauważmy, że liczba błędów nie ulega w ten sposób zmianie, a zdolność korekcyjna kodu Reeda–Mullera rzędu $r-1$ jest jeszcze większa niż odpowiednia zdolność kodu Reeda–Mullera) rzędu r.

W ten sposób wykazaliśmy, że kod Reeda–Mullera rzędu r może korygować $2^{m-r-1}-1$ błędów, zatem minimalna odległość słów kodowych wynosi $2(2^{m-r-1}-1)+1 = 2^{m-r}-1$. Jednakże wszystkie wektory kodowe mają wagę parzystą, zaś wektory $v_{i_1} \dots v_{i_r}$ wagę 2^{m-r}, a zatem minimalna waga wektorów z kodu Reeda–Mullera rzędu r wynosi 2^{m-r}.

Kody Reeda–Mullera, choć eleganckie, mają – ze względu na bardzo złożony algorytm dekodowania – niewielką użyteczność praktyczną.

Zadania

1. Ile błędów wykrywa a ile koryguje kod polegający na 4-krotnym powtórzeniu każdej litery?

2. Znaleźć słownik dla (7, 4)-kodu Hamminga, wskazać liderów warstw.

3. Znaleźć układ równań kontroli (7, 4)-kodu Hamminga.

4. Sprawdzić, że skonstruowana w § 2 macierz jest istotnie macierzą generującą (15, 11)-kod Hamminga.

5. Skonstruować kod BCH o projektowanej odległości 5, używając do tego celu elementu prymitywnego z $GF(2^5)$ spełniającego równanie $x^5+x^2+1=0$.

6. *Kodem Reeda–Solomona* (w skrócie RS) nazywamy taki kod BCH nad $GF(q)$, dla którego długość słowa kodowego wynosi $q-1$. W szczególności generator kodu RS ma postać: $g(x) = \prod_{i=1}^{d-1} (x-\alpha^i)$, gdzie α jest elementem pierwotnym, d zaś projektowaną odległością. Wykazać, że minimalna waga elementu kodu RS wynosi d.

7. Znaleźć numerator kodu BCH z zadania 5.

8. Znaleźć numerator rozszerzonego binarnego kodu Golay'a (jest to (24, 12)-kod liniowy).

9. Skonstruować (11, 6)-kod Golay'a nad $GF(3)$ używając następujących faktów (których należy dowieść):

(a) W $GF(3^5)$ istnieje element rzędu 11.

(b) $x^{11}-1=(x-1)(x^5+x^4-x^3+x^2-1)(x^5-x^3+x^2-x-1)$.

(c) Kula o promieniu 2 w $(GF(3))^{11}$ liczy 243 ($=3^5$) elementów.

(d) Definiujemy (11, 6)-kod Golay'a nad $GF(3)$ jako zbiór słów $\langle a_0, \dots, a_{10}\rangle$ takich, że $x^5+x^4-x^3+x^2-1 | a(x)$. Wykazać, że waga każdego słowa kodowego wynosi co najmniej 4.

(e) Wykazać, że jeśli $\boldsymbol{a}$ jest słowem kodowym i $\sum_{j=0}^{10} a_j = 0$, to waga $\boldsymbol{a}$ jest podzielna przez 3, jeśli zaś $\sum_{j=0}^{10} a_j \neq b \neq 0$, to każde słowo $\langle a_0+b, \dots, a_{10}+b\rangle$ jest słowem kodowym i ma wagę podzielną przez 3.

(f) Używając (e) wykazać, że skonstruowany kod nie zawiera słów wagi 4, a zatem koryguje 2 błędy.

(g) Wykazać, że skonstruowany kod jest kodem doskonałym.

10. Skonstruować za pomocą konfiguracji inny kod niż podany w §5.

11. Dla każdej macierzy Hadamarda z rozdziału 7 skonstruować odpowiadający jej kod.

12. *Produktem kodów* C_1 i C_2 ($C_1 \subseteq K^n$, $C_2 \subseteq K^m$) nazywamy następujący kod $C = C_1 \times C_2$: C jest podprzestrzenią przestrzeni K^{nm}, przy czym jeśli ustalimy reprezentację wektorów przestrzeni (nm)-wymiarowej jako macierze $n \times m$, to wiersze takiej macierzy należą do C_1, kolumny zaś do C_2.

(a) Wykazać, że $C_1 \times C_2$ jest podprzestrzenią liniową przestrzeni (nm)-wymiarowej.

(b) Wykazać, że produkt Kroneckera macierzy generujących G_1 i G_2 odpowiednio dla kodów C_1 i C_2 jest macierzą generującą dla ich produktu $C_1 \times C_2$.

(c) Wykazać, że wymiar $C_1 \times C_2$ jest równy iloczynowi wymiarów odpowiednio C_1 i C_2.

(d) Wykazać, że minimalna waga słowa w $C_1 \times C_2$ jest iloczynem minimalnych wag słów w C_1 i C_2.

13. Wykazać, że w liniowym kodzie binarnym zbiór słów o wadze parzystej tworzy podprzestrzeń. Jaki jest wymiar tej podprzestrzeni? Odpowiedź: Jeśli C jest (n, k)-kodem, to wymiar rozważanej przestrzeni wynosi k lub $k-1$.

14. Udowodnić następujące uogólnienie lematu Gleasona: Niech X będzie zbiorem skończonym, $\emptyset \neq \mathscr{H} \subseteq \mathscr{P}(X)$, $\varphi\colon \mathscr{H} \to \mathscr{H}$, $\chi\colon X^2 \to D$ będą odwzorowaniami spełniającymi następujące warunki:

Jeśli $y \in X$, $Z \in \mathscr{H}$, to

$$y \in Z \Rightarrow \text{dla każdego } x \in \varphi(Z),\ \chi(x, y) = 1,$$

$$y \notin Z \Rightarrow \sum_{x \in \varphi(Z)} \chi(x, y) = 0.$$

Niech A będzie przestrzenią liniową nad C, $f\colon X \to A$, i niech funkcja $g\colon X \to A$ będzie określona wzorem:

$$g(x) = \sum_{y \in X} \chi(y, x) f(y).$$

Wówczas dla dowolnego $Z \in \mathscr{H}$

$$\sum_{x \in Z} g(x) = |Z| \sum_{y \in \varphi(Z)} f(y).$$

CIAŁA SKOŃCZONE

W dodatku tym zebrano podstawowe fakty dotyczące ciał skończonych. Szczególny nacisk położono na konstruktywną postać samych twierdzeń, jak również ich dowodów. Od Czytelnika są wymagane jedynie zupełnie elementarne wiadomości z algebry.

Zaczniemy od przypomnienia definicji ciała. *Ciałem* będziemy nazywali dowolny zbiór F, w którym dla każdych elementów $a, b \in F$ określona jest jednoznacznie ich *suma* $a+b \in F$ oraz *iloczyn* $a \cdot b \in F$ (oznaczany zwykle ab) oraz spełnione są następujące warunki:

C1. $a+b = b+a$.

C2. $(a+b)+c = a+(b+c)$.

C3. $ab = ba$.

C4. $a(bc) = (ab)c$.

C5. $a(b+c) = ab+ac$.

C6. Istnieje element $0 \in F$, zwany *zerem* ciała F, taki, że dla każdego $a \in F$

$$a+0 = 0+a = a.$$

C7. Dla dowolnego $a \in F$ istnieje element $-a \in F$, zwany *elementem przeciwnym* do a, taki, że $a+(-a) = 0$ ($a+(-b)$ oznaczamy zwykle przez $a-b$).

C8. Istnieje element $1 \in F$ zwany *jedynką* ciała F, taki, że dla każdego $a \in F$

$$a1 = 1a = a.$$

C9. Dla dowolnego elementu $a \in F$ nie będącego zerem istnieje element $a^{-1} \in F$, zwany *elementem odwrotnym* do a, taki, że

$$aa^{-1} = a^{-1}a = 1$$

(ab^{-1} oznaczamy zwykle przez $\frac{a}{b}$ lub a/b).

C10. $0 \neq 1$.

Czytelnik z łatwością zauważy, że 0, 1 jak również element odwrotny i przeciwny dla dowolnego elementu a, są wyznaczone jednoznacznie (w ostatnim

przypadku zakładamy, że $a \neq 0$). Jest również widoczne, że warunki C1–C10 nie są niezależne, tzn. niektóre z nich wynikają z pozostałych (a więc mogłyby być pominięte).

Z warunków C1, C2, C6 i C7 wynika, że zbiór F wraz z działaniem $+$ tworzy grupę przemienną – nazywamy ją *grupą addytywną ciała F*. Podobnie warunki C3, C4, C8 i C9 mówią, że zbiór $F \setminus \{0\}$ z działaniem $\cdot$ tworzy grupę – nazywamy ją *grupą multyplikatywną* ciała F. Liczbę elementów ciała nazywamy też jego *rzędem*. Przez *podciało* ciała F rozumiemy dowolny podzbiór $E \subseteq F$, który sam jest ciałem przy działaniach $+, \cdot$ pokrywających się z odpowiednimi działaniami w F. Dwa ciała E, F są *izomorficzne*, jeśli istnieje odwzorowanie wzajemnie jednoznaczne f ciała E na ciało F, takie, że

$$f(a+b) = f(a)+f(b),$$
$$f(ab) = f(a)f(b)$$

dla dowolnych $a, b \in E$. Warunki te pociągają za sobą również warunki

$$f(0) = 0,$$
$$f(1) = 1,$$
$$f(-a) = -f(a),$$
$$f(a^{-1}) = f(a)^{-1}.$$

Jeśli $E = F$, to takie odwzorowanie f nazywamy *automorfizmem* ciała F. Jest oczywiste, że zbiór wszystkich automorfizmów ciała F z działaniem składania automorfizmów tworzy grupę.

Przykłady ciał znane każdemu to ciało $\boldsymbol{R}$ liczb rzeczywistych, ciało $\boldsymbol{C}$ liczb zespolonych oraz ciało $\boldsymbol{Q}$ liczb wymiernych. W kombinatoryce – w szczególności w teorii konfiguracji, geometrii skończonych oraz teorii kodów – podstawową rolę odgrywają jednak *ciała skończone*, tzn. ciała o skończonej liczbie elementów. Okazuje się, że liczność ciała skończonego nie może być dowolna, dokładniej, że ciało skończone rzędu q istnieje – i jest jedyne z dokładnością do izomorfizmu – wtedy i tylko wtedy, gdy q jest postaci p^m, gdzie p jest liczbą pierwszą oraz $m \geqslant 1$.

Zajmiemy się najpierw przypadkiem $m = 1$, tzn. $q = p$. W tym celu określmy w zbiorze $\boldsymbol{Z}$ liczb całkowitych *relację przystawania modulo p* następująco:

$$s \equiv t \pmod p \Leftrightarrow p \text{ dzieli } s-t.$$

Jest oczywiste, że relacja ta jest relacją równoważności, a więc określa podział zbioru $\boldsymbol{Z}$ na klasy abstrakcji postaci

$$[s] = \{t \in \boldsymbol{Z}\colon\ s \equiv t \pmod p\}$$

zwane *klasami reszt modulo p*. Co więcej, w zbiorze tych klas możemy określić działania $+, \cdot$ następująco:

(1) $$[t]+[s] = [t+s],$$

(2) $$[t]\cdot[s] = [t\cdot s].$$

Aby uzasadnić poprawność tych definicji, należy wykazać, że jeśli $[t'] = [t]$ i $[s'] = [s]$, to $[t'+s'] = [t+s]$ oraz $[t's'] = [ts]$. Wynika to jednak z poniższych elementarnych własności relacji przystawania, prawdziwych dla dowolnego $p \neq 0$ niekoniecznie będącego liczbą pierwszą:

$$t \equiv t' \pmod p \wedge s \equiv s' \pmod p \Rightarrow s+t \equiv s'+t' \pmod p,$$

$$t \equiv t' \pmod p \wedge s \equiv s' \pmod p \Rightarrow st \equiv s't' \pmod p.$$

Wykażemy, że zbiór $\boldsymbol{Z}_p$ wszystkich klas reszt modulo p wraz z działaniami $+, \cdot$ określonymi przez (1) i (2) tworzy ciało o p elementach. Jest oczywiste, że $\boldsymbol{Z}_p$ zawiera dokładnie p elementów – możemy je przedstawić jako $[0], [1], \ldots, [p-1]$. Bezpośrednim wnioskiem z definicji (1), (2) jest to, że działania $+, \cdot$ w $\boldsymbol{Z}_p$ spełniają warunki C1–C8, przy czym rolę zera odgrywa $[0]$, a rolę jedności $[1]$. Wynika to z oczywistego faktu, że warunki te są spełnione dla zbioru $\boldsymbol{Z}$ liczb całkowitych. Warunek C10 jest spełniony, jeśli tylko $p \neq 1$. Jedynym warunkiem, przy sprawdzaniu którego będziemy korzystali z faktu, że p jest liczbą pierwszą, jest C9. Zauważmy, że dla p złożonego, np. $p = 6$, mamy $[2][3] = [6] = [0]$, podczas gdy ani $[2]$ ani $[3]$ nie jest elementem zerowym w $\boldsymbol{Z}_6$. O niezerowych elementach a, b takich, że $ab = 0$, mówimy, że są *dzielnikami zera*. Żadne ciało nie może zawierać dzielników zera, gdyż jeśli $a \neq 0$, to równość $ab = 0$ jest równoważna $a^{-1}ab = a^{-1}0$, czyli $b = 0$. Tak więc $\boldsymbol{Z}_6$ z działaniami określonymi przez (1), (2) nie jest ciałem, podobnie jak nie jest ciałem Z_r dla żadnej złożonej liczby r. Jeśli jednak p jest liczbą pierwszą, to warunek C9 jest spełniony. Aby to wykazać, ustalmy dowolną liczbę $t \not\equiv 0 \pmod p$ i rozważmy liczby

(3) $$t \cdot 1,\ t \cdot 2,\ \ldots,\ t(p-1)$$

Zauważmy, że jeśli $ti \equiv tj \pmod p$, $1 \leqslant i < j \leqslant p-1$, to $t(j-i) \equiv 0 \pmod p$ i w konsekwencji $i = j$. Korzystamy tu z następującej własności liczb pierwszych: jeśli $p|ts$, to $p|t$ lub $p|s$. Z tej samej własności wynika, że p nie dzieli żadnej z liczb (3). Zatem każda z nich wpada do innej spośród niezerowych klas reszt modulo p. Tych niezerowych klas jest $p-1$, tyle co liczb (3). Tak więc do każdej klasy musi wpadać dokładnie jedna liczba. W szczególności $ts \in [1]$ dla pewnego s, $1 \leqslant s \leqslant p-1$. Mamy zatem $[t][s] = [1]$, tzn. $[s]$ jest odwrotnością elementu $[t]$. Tym samym warunek C9 jest spełniony i otrzymujemy następujące twierdzenie.

TWIERDZENIE 1. *Jeśli p jest liczbą pierwszą (i tylko wtedy), to zbiór $\boldsymbol{Z}_p$ klas reszt modulo p wraz z działaniami określonymi przez* (1), (2) *tworzy ciało o p elementach.* □

Ciało to nazywamy *ciałem reszt modulo p* lub *ciałem Galois rzędu p* i oznaczamy zwykle przez $GF(p)$ (od ang. *Galois field*). Zwykle klasę $[t]$ reprezentujemy przez resztę z dzielenia t przez p, tzn. jedyną liczbę $s \equiv t \pmod p$ spełniającą nierówności $0 \leqslant s \leqslant p-1$. Tę liczbę s oznaczamy czasem przez $t \pmod p$. Przy takiej reprezentacji działania w $GF(p)$ wykonujemy tak jak zwykłe działania na liczbach, z tym że wynik należy zredukować modulo p.

Najprostszym ciałem Galois jest $GF(2)$. Składa się ono z elementów 0 i 1, przy czym działania określone są następująco:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Warto zauważyć, że w ciele tym mamy zawsze $-a = a$ oraz $a^n = a$ dla dowolnego n. Ciało $GF(3)$ możemy reprezentować przez elementy 0, 1, 2 z następującymi działaniami:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Moglibyśmy również elementy ciała $GF(3)$ reprezentować przez 0, 1, -1. Odpada wtedy konieczność dokonywania redukcji modulo 3 po wykonaniu mnożenia.

Niech 1 będzie jednością pewnego ciała skończonego F. Razem z jednością F zawiera elementy

$$1+1 = \sum_{i=1}^{2} 1, \quad 1+1+1 = \sum_{i=1}^{3} 1, \quad \ldots, \quad 1+\ldots+1 = \sum_{i=1}^{n} 1, \ldots$$

zwane *liczbami* ciała F. Ciało F jest skończone, muszą zatem istnieć liczby naturalne m, n takie, że $m > n \geqslant 0$ oraz $\sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1$, tzn. $\sum_{i=1}^{m-n} 1 = 0$. Najmniejszą spośród liczb dodatnich k takich, że $\sum_{i=1}^{k} 1 = 0$ nazywamy *charakterystyką* ciała F. Zbiór liczb ciała jest oczywiście zamknięty ze względu na dodawanie, jest również zamknięty ze względu na mnożenie, gdyż wobec rozdzielności mnożenia względem dodawania mamy

$$\left(\sum_{i=1}^{m} 1\right)\left(\sum_{i=1}^{n} 1\right) = \sum_{i=1}^{mn} (1 \cdot 1) = \sum_{i=1}^{mn} 1.$$

Jeśli $\sum_{i=1}^{mn} 1 = 0$, to $\sum_{i=1}^{m} 1 = 0$ lub $\sum_{i=1}^{n} 1 = 0$, gdyż – jak już zauważyliśmy – ciało nie może zawierać dzielników zera. Otrzymujemy stąd następujący wniosek:

TWIERDZENIE 2. *Charakterystyka dowolnego ciała skończonego jest liczbą pierwszą.* □

Oczywiście dla dowolnej liczby pierwszej p charakterystyka ciała $GF(p)$ jest równa p.

TWIERDZENIE 3. *Zbiór liczb dowolnego ciała skończonego o charakterystyce p tworzy podciało izomorficzne z $GF(p)$.*

Dowód. Żądany izomorfizm określamy przyporządkowując reszcie $t \pmod p$ liczbę $\sum_{i=1}^{t} 1$ ciała F. □

Podciało złożone z liczb ciała F nazywamy czasem *podciałem prostym* ciała F.

Pokażemy teraz metodę pozwalającą skonstruować dla każdego $m \geqslant 1$ ciało rzędu q^m mając dane ciało rzędu q. Skonstruowaliśmy już ciało rzędu p, gdzie p jest dowolną liczbą pierwszą, tak więc otrzymamy w ten sposób ciała rzędu p^m, $m \geqslant 1$. Okazuje się, że ciała o innej liczbie elementów nie istnieją. Wynika to z następującego prostego lematu.

LEMAT 4. *Jeśli E jest podciałem ciała skończonego F, to rząd ciała F jest potęgą rzędu ciała E.*

Dowód. Jeśli traktować elementy ciała E jako „skalary", elementy ciała F zaś jako „wektory", to – przy działaniach mnożenia wektora przez skalar oraz dodawania wektorów określonych przez działania $\cdot$, $+$ w ciele F – spełnione są wszystkie aksjomaty przestrzeni liniowej. Tak więc F jest przestrzenią liniową nad ciałem E. Oznaczmy przez m wymiar tej przestrzeni, przez q zaś rząd ciała E. Każdy element $a \in F$ ma jednoznaczne rozwinięcie

$$\sum_{i=1}^{m} a_i b_i, \tag{4}$$

gdzie $b_1, \ldots, b_m$ jest pewną bazą naszej przestrzeni oraz $a_1, \ldots, a_m \in E$. Tak więc elementów ciała F jest dokładnie tyle, ile rozwinięć postaci (4), tzn. q^m. □

Przyjmując jako E podciało proste ciała F otrzymujemy jako wniosek następujące twierdzenie.

TWIERDZENIE 5. *Niech F będzie ciałem skończonym o charakterystyce p. Wówczas rząd ciała F jest postaci p^m, $m \geqslant 1$, rząd zaś dowolnego podciała $E \subseteq F$ jest postaci p^n, gdzie $n|m$.*

Dowód. Na mocy poprzedniego twierdzenia $p^m = (p^n)^k = p^{nk}$, czyli $m = nk$ dla pewnego k. □

Do zapowiedzianej konstrukcji ciała rzędu q^m z ciała rzędu q potrzebne nam będą pewne elementarne wiadomości dotyczące wielomianów. Będziemy rozważali wielomiany jednej zmiennej nad dowolnym ciałem F rzędu q (tzn. o współczynnikach z ciała F). *Stopień wielomianu* $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$, tzn. największą z liczb k, dla których $a_k \neq 0$, będziemy oznaczali przez $\deg P$. Jeśli

dodatkowo określimy $\deg 0 = -\infty$, to dla dowolnych wielomianów P, Q mamy

(5) $$\deg(P+Q) \leqslant \max(\deg P, \deg Q),$$

(6) $$\deg(PQ) = \deg P + \deg Q.$$

Wielomian n-tego stopnia $P(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ jest *unormowany*, jeśli $a_n = 1$.

Wielomiany mają własności podobne pod wieloma względami do własności liczb całkowitych. Zauważmy na początek, że dodawanie i mnożenie wielomianów spełnia warunki C1–C10 oprócz warunku C9, to znaczy wielomiany – podobnie jak liczby całkowite – tworzą pierścień przemienny z jedynką. Na mocy wzoru (6) w pierścieniu wielomianów nie ma dzielników zera. Wynika stąd następujące prawo skracania: Jeśli $P \neq 0$ i $PQ = PR$, to $Q = R$. W pierścieniu wielomianów można również określić dzielenie z resztą, korzystając z faktu, iż dla dowolnych wielomianów P, Q istnieją wielomiany A, R takie, że

(7) $$P = AQ + R, \qquad \deg R < \deg Q.$$

Wielomiany A i R można otrzymać używając znanego algorytmu dzielenia wielomianów. Poniższy przykład ilustruje dzielenie dwóch wielomianów nad $GF(2)$: $x^5 + x^2$ przez $x^2 + 1$:

$$\begin{array}{llll}
 & x^3 & +x+1 & \\
\hline
x^5 & & +x^2 & : x^2+1 \\
x^5 & +x^3 & & \\
\hline
 & x^3 & +x^2 & \\
 & x^3 & +x & \\
\hline
 & & x^2+x & \\
 & & x^2 \quad +1 & \\
\hline
 & & x+1 &
\end{array}$$

Otrzymaliśmy wynik

$$x^5 + x^2 = (x^3 + x + 1)(x^2 + 1) + (x + 1).$$

Wielomiany A i R we wzorze (7) są jednoznacznie wyznaczone przez P, Q. Jeśli bowiem

(8) $$P = A'Q + R', \qquad \deg R' < \deg Q,$$

to odejmując stronami (7) od (8) otrzymujemy

$$0 = (A - A')Q + (R - R'),$$

a stąd, wobec $\deg(R - R') < \deg Q$, otrzymujemy natychmiast $A' = A$, $R' = R$. Wielomian R nazywamy *resztą z dzielenia P przez Q*.

Dużo informacji dotyczących własności wielomianów daje tzw. *algorytm Euklidesa*. Aby go opisać załóżmy, że dane są dowolne dwa wielomiany P, Q. Określmy

(9) $$R_1 = P, \quad R_2 = Q,$$

(10) $$P_1 = 0, \quad P_2 = 1,$$

(11) $$Q_1 = 1, \quad Q_2 = 0.$$

Zaczynając od tych sześciu wielomianów będziemy obliczali dla $i = 3, 4, 5, \ldots$ wielomiany R_i, A_i, P_i, Q_i spełniające równości

(12) $$R_{i-2} = A_i R_{i-1} + R_i, \qquad \deg R_i < \deg R_{i-1},$$

(13) $$R_i = A_i P_{i-1} + P_{i-2},$$

(14) $$Q_i = A_i Q_{i-1} + Q_{i-2}.$$

Obliczenia przerywamy, gdy $R_n = 0$ — do tej sytuacji zawsze dojdzie, gdyż ciąg $\deg R_2$, $\deg R_3$, $\deg R_4, \ldots$ jest ściśle malejący. Wzory (12), (13), (14) wraz z warunkami początkowymi (9), (10), (11) określają jednoznacznie ciągi wielomianów

$$R_1, R_2, \ldots, R_n, \quad P_1, P_2, \ldots, P_n, \quad Q_1, Q_2, \ldots, Q_n.$$

Istotnie wielomian R_i jest na mocy wzoru (12) resztą z dzielenia R_{i-2} przez R_{i-1}, wzory zaś (13) i (14) bezpośrednio określają P_i jako funkcję P_{i-2}, P_{i-1} oraz Q_i jako funkcję Q_{i-2}, Q_{i-1}. Ze wzoru (12) wynika bezpośrednio następująca równoważność dla dowolnego wielomianu W:

(15) $$W \text{ dzieli } R_{i-2} \text{ i } R_{i-1} \Leftrightarrow W \text{ dzieli } R_{i-1} \text{ i } R_i$$

$(3 \leqslant i \leqslant n)$. Stąd wynika natychmiast, że

(16) $$W \text{ dzieli } R_1 \text{ i } R_2 \Leftrightarrow W \text{ dzieli } R_{n-1} \text{ i } R_n.$$

Uwzględniając równości (9) oraz fakt, że $R_n = 0$ otrzymujemy ostatecznie równoważność

$$W \text{ dzieli } P \text{ i } Q \Leftrightarrow W \text{ dzieli } R_{n-1}.$$

Tak więc wielomian R_{n-1} dzieli P i Q oraz każdy wielomian W maksymalnego stopnia dzielący P i Q ma postać aR_{n-1}, gdzie $a \in F$. Możemy zatem jednoznacznie określić *największy wspólny dzielnik* wielomianów P i Q jako znormalizowany wielomian największego stopnia dzielący P i Q. Będziemy go oznaczali przez (P, Q). Aby obliczyć (P, Q), wystarczy zastosować algorytm Euklidesa a następnie unormować R_{n-1}, tzn. podzielić przez współczynnik przy najwyższej potędze. O wielomianach P, Q będziemy mówili, że są *względnie pierwsze*, jeśli $(P, Q) = 1$.

Zajmiemy się teraz wielomianami P_i, Q_i. Ze wzorów (12) (13), (14) wynikają następujące trzy zależności:

$$Q_iR_{i+1}+Q_{i+1}R_i = Q_i(-A_{i+1}R_i+R_{i-1})+(A_{i+1}Q_i+Q_{i-1})R_i = Q_{i-1}R_i+Q_iR_{i-1}, \tag{17}$$

$$P_iR_{i+1}+P_{i+1}R_i = P_i(-A_{i+1}R_i+R_{i-1})+(A_{i+1}P_i+P_{i-1})R_i = R_{i-1}R_i+R_iR_{i-1}, \tag{18}$$

$$Q_{i+1}P_i-P_{i+1}Q_i = (A_{i+1}Q_i+Q_{i-1})P_i-(A_{i+1}P_i+P_{i-1})Q_i = -(Q_iP_{i-1}-P_iQ_{i-1}). \tag{19}$$

Przez rozumowanie indukcyjne — podobne do zastosowanego przy wyprowadzeniu (16) z (15) — otrzymujemy z (17), (18), (19) następujące zależności:

$$Q_1R_2+Q_2R_1 = Q_{n-1}R_n+Q_nR_{n-1},$$
$$P_1R_2+P_2R_1 = P_{n-1}R_n+P_nR_{n-1},$$
$$Q_2P_1-P_2Q_1 = (-1)^{n-2}(Q_nP_{n-1}-P_nQ_{n-1}),$$

czyli, po uwzględnieniu wzorów (9), (10), (11),

$$Q = Q_nR_{n-1}, \tag{20}$$

$$P = P_nR_{n-1}, \tag{21}$$

$$1 = (-1)^n(P_nQ_{n-1}-Q_nP_{n-1}). \tag{22}$$

Jeśli tę ostatnią równość pomnożymy stronami przez R_{n-1} i skorzystamy z dwóch poprzednich równości, to otrzymamy

$$R_{n-1} = (-1)^n(Q_{n-1}P-P_{n-1}Q). \tag{23}$$

Mamy stąd następujący wniosek:

WNIOSEK 6. *Dla dowolnych wielomianów P, Q istnieją wielomiany A, B takie, że*

$$AP+BQ = (P, Q). \ \square$$

O wielomianie P będziemy mówili, że jest *nierozkładalny nad ciałem F*, jeśli P jest wielomianem nad F oraz nie istnieją wielomiany Q, R nad ciałem F takie, że $P = QR$, $\deg Q < \deg P$ i $\deg R < \deg P$. Wniosek 6 posłuży nam do dowodu następującej ważnej analogii pomiędzy liczbami pierwszymi a wielomianami nierozkładalnymi.

LEMAT 7. *Jeśli wielomian P nierozkładalny nad ciałem F dzieli iloczyn dwóch wielomianów A, B nad F, to P dzieli A lub P dzieli B.*

Dowód. Załóżmy, że P nie dzieli wielomianu A. Wtedy, wobec nierozkładalności wielomianu P, mamy $(P, A) = 1$. Na mocy wniosku 6 istnieją wielomiany C,

D takie, że $CP+DA = 1$, czyli $CPB+DAB = B$. Lecz P dzieli oba składniki lewej strony ostatniej równości, a więc dzieli też wielomian B. □

Z lematu tego wynika natychmiast następujące twierdzenie będące odpowiednikiem twierdzenia o jednoznaczności rozkładu dowolnej liczby naturalnej na iloczyn liczb pierwszych.

TWIERDZENIE 8. *Każdy znormalizowany wielomian stopnia większego od zera rozkłada się jednoznacznie — z dokładnością do porządku czynników — na iloczyn znormalizowanych wielomianów nierozkładalnych stopni większych od zera.*

Dowód. Jeśli

$$A_1 \dots A_m = B_1 \dots B_n$$

są dwoma rozkładami, to na mocy nierozkładalności i lematu 7 każdy wielomian A_i dzieli pewien wielomian B_j. Lecz oba te wielomiany są znormalizowane, B_j zaś jest nierozkładalny, zatem $A_i = B_j$. Rozumowanie to powtarzamy dla równości

$$A_1 \dots A_{i-1}A_{i+1} \dots A_m = B_1 \dots B_{j-1}B_{j+1} \dots B_n$$

itd., aż do wyczerpania wszystkich czynników. □

Każdy wielomian P nad ciałem F możemy przedstawić jako

$$P = aA_1 \dots A_n,$$

gdzie $a \in F$ oraz $A_1, \dots, A_n$ są znormalizowanymi wielomianami nierozkładalnymi nad F, $\deg A_i > 0$, $n \geqslant 0$. Przedstawienie takie jest jedyne, z dokładnością do porządku czynników. Nazywamy je *rozkładem kanonicznym wielomianu P nad ciałem F*. Rozkład kanoniczny nad większym ciałem $E \supseteq F$ zawiera na ogół większą liczbę czynników, gdyż pewne czynniki A_i rozpadają się na iloczyn czynników nierozkładalnych nad E.

Jeśli wielomian $P(x)$ ma pierwiastek a, to $x-a$ dzieli $P(x)$. Istotnie, przedstawiając $P(x)$ jako $A(x)(x-a)+c$, gdzie c jest resztą z dzielenia $P(x)$ przez $x-a$, i przyjmując $x = a$ otrzymujemy $c = 0$. Tak więc liczba pierwiastków wielomianu jest równa liczbie czynników pierwszego stopnia w jego rozkładzie na czynniki nierozkładalne. W konsekwencji liczba pierwiastków wielomianu nie może przekraczać jego stopnia. Odnotujmy ten fakt jako następujący

LEMAT 9. *Każdy wielomian n-tego stopnia nad ciałem F ma w dowolnym ciele $E \supseteq F$ co najwyżej n pierwiastków.* □

Dla dowolnego wielomianu P nad ciałem F określamy w zbiorze wszystkich wielomianów nad F *relację przystawania modulo P* następująco:

$$A \equiv B \pmod{P} \Leftrightarrow P \text{ dzieli } A-B.$$

Podobnie jak w przypadku przystawania liczb łatwo sprawdzamy, że jest to relacja równoważności, oraz że w zbiorze jej klas równoważności — zwanych *klasami*

reszt modulo P — możemy określić działania $+, \cdot$ wzorami

(24) $$[A]+[B]=[A+B],$$

(25) $$[A]\cdot[B]=[A\cdot B],$$

gdzie

$$[A]=\{B\colon A\equiv B \pmod P\}.$$

Zapowiedziana konstrukcja ciała rzędu q^m z ciała rzędu q oparta jest na następującym twierdzeniu.

TWIERDZENIE 10. *Jeśli P jest wielomianem nierozkładalnym stopnia m nad ciałem F rzędu q, to klasy reszt modulo P z działaniami określonymi wzorami* (24), (25) *tworzą ciało rzędu* q^m.

Dowód. Wszystkich klas jest tyle, ile jest możliwych reszt z dzielenia przez P. Każda taka reszta jest pewnym wielomianem stopnia mniejszego niż m, tzn. jest postaci $\sum_{i=0}^{m-1} a_i x^i$, gdzie $a_i \in F$. Każdy spośród m współczynników może przyjmować q wartości, zatem wielomianów tych — a więc i klas reszt modulo P — jest dokładnie q^m. Klasy te z działaniami $+, \cdot$ określonymi przez (24) i (25) tworzą pierścień przemienny z jedynką. Wynika to bezpośrednio ze sposobu, w jaki określiliśmy działania na klasach, i z faktu, że wielomiany tworzą pierścień przemienny z jedynką. Pozostaje jedynie do wykazania istnienie elementu odwrotnego (warunek C9). Ustalmy dowolny wielomian $A \not\equiv 0 \pmod P$ i rozważmy q^m-1 wielomianów postaci

(26) $$AW, \quad \deg W < m, \quad W \neq 0.$$

Wykażemy, że wszystkie te wielomiany wyznaczają różne klasy reszt modulo P. Istotnie, jeśli $AW_1 \equiv AW_2 \pmod P$, to P dzieli $A(W_1-W_2)$. Lecz P jest wielomianem nierozkładalnym oraz P nie dzieli A. Z lematu 7 wynika, że P dzieli W_1-W_2, a z nierówności $\deg(W_1-W_2) < \deg P$, że $W_1 = W_2$. Podobnie, z nierozkładalności wielomianu P wynika, że żaden z iloczynów (26) nie jest podzielny przez P.

Skoro każdy z q^m-1 wielomianów (26) wpada do innej spośród q^m-1 niezerowych klas reszt modulo P, to dla pewnego wielomianu W mamy $AW \equiv 1 \pmod P$, tzn. $[W]$ jest odwrotnością $[A]$. Dowód jest tym samym zakończony. □

Widzimy, że dowód przebiegał analogicznie jak w przypadku twierdzenia 1. Pierścieniowi liczb całkowitych odpowiada pierścień wielomianów, zaś liczbie pierwszej p wielomian nierozkładalny P. Ciało, które skonstruowaliśmy, będziemy nazywali *ciałem reszt modulo P nad F*.

Zwykle klasę A reprezentujemy przez resztę z dzielenia A przez P. Resztę tę oznaczamy czasem przez $A \pmod P$. Przy takiej reprezentacji ciało skonstruowane

w twierdzeniu 10 składa się ze wszystkich wielomianów nad F stopnia mniejszego niż m, działania zaś wykonujemy tak jak zwykłe działania na wielomianach, z tym że wynik mnożenia należy zawsze redukować modulo P.

Dla przykładu skonstruujemy ciało o $2^2 = 4$ elementach. Potrzebny nam będzie wielomian stopnia drugiego nierozkładalny nad $GF(2)$. Takim wielomianem x^2+x+1. Istotnie, nie jest on iloczynem dwóch wielomianów stopnia mniejszego niż 2, tzn. stopnia pierwszego, gdyż jedynymi takimi wielomianami są x i $x+1$, zaś

$$x \cdot x = x^2,$$

$$x(x+1) = x^2+x,$$

$$(x+1)(x+1) = x^2+2x+1.$$

Elementy naszego ciała możemy reprezentować przez

$$0,\ 1,\ x,\ x+1.$$

Mamy

$$x^2 (\operatorname{mod} x^2+x+1) = x+1,$$

$$x(x+1)(\operatorname{mod} x^2+x+1) = 1,$$

$$(x+1)(x+1)(\operatorname{mod} x^2+x+1) = x,$$

tak więc działania w naszym ciele można przedstawić następująco:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Konstrukcję w dowodzie twierdzenia 10 przeprowadziliśmy przy założeniu istnienia wielomianu nierozkładalnego stopnia m. Wykażemy teraz, że dla dowolnego $m \geqslant 1$ oraz dowolnego ciała skończonego F istnieje co najmniej jeden wielomian nierozkładalny nad F stopnia m. Ponieważ z kontekstu będzie zawsze wynikać jakie ciało F mamy na myśli, będziemy oznaczali liczbę znormalizowanych wielomianów nierozkładalnych nad F przez I_m. Idea wyznaczania wartości I_m, jaką zastosujemy, jest następująca. Znając wartości $I_1, I_2, \ldots, I_{m-1}$ możemy wyznaczyć liczbę wszystkich rozkładów wielomianów unormowanych stopnia m na czynniki unormowane stopni mniejszych niż m. Na mocy jednoznaczności rozkładu liczbę I_m otrzymujemy jako różnicę między liczbą wszystkich wielomianów unormowanych stopnia m (tzn. q^m, gdzie q jest rzędem ciała F) a obliczoną przez nas liczbą rozkładów. Z definicji każdy wielomian stopnia pierwszego jest nierozkładalny, zatem I_1 wynosi q, tyle ile jest wszystkich wielomianów unormowanych stopnia pierwszego. Obliczymy najpierw parę początkowych wartości w przypadku $F =$

$= GF(2)$ (w tym przypadku każdy wielomian jest „automatycznie" unormowany). Mamy $I_1 = q = 2$. Wielomian stopnia drugiego może się rozkładać na 3 sposoby na czynniki stopnia pierwszego:

$$xx,\ x(x+1),\ (x+1)(x+1).$$

Ponieważ mamy $2^2 = 4$ wielomiany unormowane drugiego stopnia, więc $I_2 = 4-3 = 1$. Pdobnie, wielomian trzeciego stopnia może się rozkładać na czynniki nierozkładalne w następujący sposób:

3 czynniki liniowe, 4 sposoby

1 czynnik liniowy, 1 kwadratowy, $I_1 I_2 = 2$ sposoby.

Stąd $I_3 = 2^3 - (4+2) = 2$.

Dla wyprowadzenia ogólnego wzoru na I_m skorzystamy z metody funkcji tworzących (p. rozdział 3). Dowolnemu zbiorowi wielomianów S, zawierającemu dla każdego $k \geqslant 0$ tylko skończoną liczbę a_k wielomianów stopnia k, przyporządkujemy funkcję tworzącą ciągu $a_0, a_1, a_2, \ldots$, tzn. szereg formalny

$$\sum_{i=0}^{\infty} a_i x^i.$$

Szereg ten będziemy nazywali *numeratorem* zbioru S. Niech $S_1, \ldots, S_k$ będą zbiorami wielomianów, zaś

$$A^{(1)}(x) = \sum_{i=0}^{\infty} a_i^{(1)} x^i, \quad \ldots, \quad A^{(k)}(x) = \sum_{i=0}^{\infty} a_i^{(k)} x^i$$

ich numeratorami. Jeśli założymy, że każde dwa wielomiany $P \in S_i$, $Q \in S_j$, $i \neq j$, są względnie pierwsze, to każdy wielomian W ze zbioru

$$S = \{P_1 P_2 \ldots P_k\colon\ P_1 \in S_1 \wedge \ldots \wedge P_k \in S_k\}$$

daje się jednoznacznie przedstawić jako $W = P_1 P_2 \ldots P_k$, gdzie $P_i \in S_i$ dla $1 \leqslant i \leqslant k$. Numerator $A(x) = \sum_{i=0}^{\infty} a_i x^i$ zbioru S ma wtedy postać

(27) $$A(x) = A^{(1)}(x) \ldots A^{(k)}(x).$$

Istotnie, każdy wielomian stopnia r w S jest (na dokładnie jeden sposób) iloczynem

(28) $$P_1 P_2 \ldots P_k, \quad \text{gdzie } P_i \in S_i \quad \text{dla } 1 \leqslant i \leqslant k.$$

Dla każdego podziału $r = r_1 + \ldots + r_k$ ($r_i \geqslant 0$ dla $1 \leqslant i \leqslant k$) mamy dokładnie $a_{r_1}^{(1)} a_{r_2}^{(2)} \ldots a_{r_k}^{(k)}$ iloczynów postaci (28) takich, że $\deg P_i = r_i$ dla $1 \leqslant i \leqslant k$. Tak więc

$$a_r = \sum a_{r_1}^{(1)} a_{r_2}^{(2)} \ldots a_{r_k}^{(k)},$$

gdzie sumowanie rozciąga się na wszystkie podziały $r = r_1 + \ldots + r_k$. Jest to jednak nic innego jak równoważny zapis równości (27).

Zauważmy teraz, że dla dowolnego wielomianu P stopnia m numerator zbioru $\{P^i\colon i \geqslant 0\}$ jest równy

$$1+x^m+x^{2m}+\ldots = \frac{1}{1-x^m}. \tag{29}$$

Liczba znormalizowanych wielomianów stopnia k nad ciałem F rzędu q jest równa q^k, a zatem numerator zbioru wszystkich unormowanych wielomianów nad F jest równy

$$1+qx+q^2x^2+q^3x^3+\ldots = \frac{1}{1-qx}. \tag{30}$$

Twierdzenie 11. *Niech I_m oznacza liczbę unormowanych wielomianów nierozkładalnych stopnia m nad ciałem F rzędu q. Wtedy*

$$\frac{1}{1-qx} = \prod_{m=1}^{\infty}\left(\frac{1}{1-x^m}\right)^{I_m}. \tag{31}$$

Dowód. Na mocy poprzednich uwag wystarczy wykazać, że prawa strona równości (31) jest numeratorem zbioru S wszystkich unormowanych wielomianów nad ciałem F. Ustawmy wszystkie unormowane wielomiany nierozkładalne nad F w ciąg $P_1, P_2, P_3, \ldots$, w którym najpierw występują wszystkie wielomiany stopnia pierwszego, potem stopnia drugiego itd. Oznaczmy przez S_i zbiór potęg wielomianu P_i, tzn. $S_i = \{P_i^k\colon k \geqslant 0\}$. Zgodnie ze wzorem (29) numerator zbioru S_i jest równy $1/(1-x^{r_i})$, gdzie $r_i = \deg P_i$. Na mocy twierdzenia 7 każdy wielomian $W \in S$ możemy przedstawić jednoznacznie jako iloczyn nieskończony $Q_1Q_2\ldots$, gdzie $Q_i \in S_i$ dla każdego $i \geqslant 1$ oraz $Q_i \neq 1$ tylko dla skończonej liczby wskaźników i. Rozumując analogicznie jak w przypadku skończonej liczby czynników (por. wzór (27)) dochodzimy do wniosku, że numerator zbioru S jest iloczynem nieskończonym numeratorów zbioru S_i, tzn. jest równy

$$\prod_{i=1}^{\infty}\frac{1}{1-x^{r_i}}.$$

Grupując czynniki odpowiadające tym samym wartościom r_i oraz uwzględniając fakt, że jest dokładnie I_m czynników S_i, dla których $r_i = m$, iloczyn ten możemy przekształcić do postaci

$$\prod_{m=1}^{\infty}\left(\frac{1}{1-x^m}\right)^{I_m}. \quad \square$$

Równość (31) posłuży nam do wyznaczenia wartości I_m. Najpierw udowodnimy następujący lemat

Lemat 12. *Dla dowolnego $k \geqslant 1$*

$$q^k = \sum_{m\colon m|k} mI_m. \tag{32}$$

Dowód. Biorąc odwrotność obu stron równości (31) otrzymujemy

$$1-qx=\prod_{j=1}^{\infty}(1-x^j)^{I_j}. \tag{33}$$

Po zróżniczkowaniu obu stron dostajemy

$$-q=\sum_{m=1}^{\infty}\frac{-mx^{m-1}I_m(1-x^m)^{I_m-1}}{(1-x^m)^{I_m}}\prod_{j=1}^{\infty}(1-x^j)^{I_m}=$$
$$=\sum_{m=1}^{\infty}\frac{-mx^{m-1}I_m}{1-x^m}\prod_{j=1}^{\infty}(1-x^j)^{I_j}.$$

Równość ta po podzieleniu stronami przez (33) a następnie pomnożeniu obu stron przez $-x$ przyjmuje postać

$$\frac{qx}{1-qx}=\sum_{m=1}^{\infty}mI_m\frac{x^m}{1-x^m}.$$

Korzystając z równości

$$\frac{qx}{1-qx}=\sum_{k=1}^{\infty}q^kx^k,$$
$$\frac{x^m}{1-x^m}=\sum_{i=1}^{\infty}x^{im}=\sum_{k:\,m|k}x^k$$

otrzymujemy ostatecznie

$$\sum_{k=1}^{\infty}q^kx^k=\sum_{m=1}^{\infty}mI_m\sum_{k:\,m|k}x^k=\sum_{k=1}^{\infty}\sum_{m:\,m|k}mI_mx^k.$$

Żądana równość (32) wynika stąd przez porównanie współczynników przy x^k. □

Z lematu 12 możemy od razu wyznaczyć I_m korzystając ze wzoru inwersyjnego Möbiusa (p. rozdział 2, wzór (5.11)). Otrzymujemy

WNIOSEK 13. *Dla dowolnego* $m\geqslant 1$

$$I_m=\frac{1}{m}\sum_{k:\,k|m}\mu(k)q^{m/k}, \tag{34}$$

gdzie μ *jest teorio-liczbową funkcją Möbiusa.* □

Przypomnijmy, że

$$\mu(k)=\begin{cases}1, & \text{jeśli } k=1,\\ (-1)^r, & \text{jeśli } k \text{ jest iloczynem } r \text{ różnych liczb pierwszych},\\ 0, & \text{jeśli } t^2|k \text{ dla pewnego } t>1\end{cases}$$

i wyznaczmy parę początkowych wartości I_m:

$$I_1 = \tfrac{1}{1}\mu(1)q = q,$$
$$I_2 = \tfrac{1}{2}\big(\mu(1)q^2 + \mu(2)q\big) = \tfrac{1}{2}(q^2 - q),$$
$$I_3 = \tfrac{1}{3}\big(\mu(1)q^3 + \mu(3)q\big) = \tfrac{1}{3}(q^3 - q),$$
$$I_4 = \tfrac{1}{4}\big(\mu(1)q^4 + \mu(2)q^2 + \mu(4)q\big) = \tfrac{1}{4}(q^4 - q^2),$$
$$I_5 = \tfrac{1}{5}\big(\mu(1)q^5 + \mu(5)q\big) = \tfrac{1}{5}(q^5 - q),$$
$$I_6 = \tfrac{1}{6}\big(\mu(1)q^6 + \mu(2)q^3 + \mu(3)q^2 + \mu(6)q\big) = \tfrac{1}{6}(q^6 - q^3 - q^2 + q).$$

Dominującym składnikiem w sumie (34) jest $\frac{1}{m}\mu(1)q^m = \frac{1}{m}q^m$. Istotnie, biorąc pod uwagę fakt, że liczba m ma mniej niż m dzielników $k \neq 1$, oraz że dla każdego takiego dzielnika $m/k \leqslant m/2$, otrzymujemy oszacowanie

$$I_m > \frac{1}{m}(q^m - qq^{m/2}) = \frac{1}{m}(q^m - q^{m/2+1}). \tag{35}$$

Wynika stąd, że $I_m > 0$ dla $m > 1$. Lecz $I_1 = q > 0$, zatem mamy następujące twierdzenie.

TWIERDZENIE 14. *Dla każdego ciała skończonego F i dowolnej liczby naturalnej $m > 0$ istnieje wielomian nierozkładalny stopnia m nad F.* □

Możemy łatwo uzyskać asymptotyczne oszacowanie liczb I_m. Zauważmy w tym celu, że z (32) wynika nierówność $q^m \geqslant I_1 + mI_m = q + mI_m$, tzn. $I_m \leqslant \frac{1}{m}(q^m - q)$ (nierówność ta przechodzi w równość, jeśli m jest liczbą pierwszą). W połączeniu z dolnym oszacowaniem (35) prowadzi to do następującego wniosku:

$$I_m \approx \frac{1}{m}q^m.$$

Innymi słowy, asymptotycznie $1/m$ unormowanych wielomianów stopnia m – a więc także $1/m$ wszystkich wielomianów stopnia m – jest nierozkładalnych.

Z twierdzeń 10 i 5 otrzymujemy bezpośrednio następujący

WNIOSEK 15. *Ciało rzędu q istnieje wtedy i tylko wtedy, gdy $q = p^m$, gdzie p jest liczbą pierwszą, m zaś dowolną liczbą naturalną.* □

Zajmiemy się teraz bliżej strukturą grupy multyplikatywnej ciał skończonych. Niech a będzie dowolnym niezerowym elementem ciała skończonego F. Rozważmy ciąg $a, a^2, a^3, \ldots$, gdzie a^n definiujemy indukcyjnie dla dowolnej liczby całkowitej n następująco: $a^0 = 1$, $a^{i+1} = aa^i$, $a^{-i} = 1/a^i$. Ze względu na skończoność ciała F muszą istnieć liczby m, n takie, że $m > n$ oraz $a^m = a^n$, tzn. $a^{m-n} = 1$. Najmniejszą z liczb $k \geqslant 1$, dla których $a^k = 1$ nazywamy *rzędem multyplikatywnym* – lub po prostu *rzędem* – elementu a. Element rzędu r nazywamy też czasem *pierwiastkiem*

pierwotnym stopnia r z jedności. Rzędu elementu 0 nie definiujemy. Jeśli r jest rzędem elementu a, to wszystkie wyrazy ciągu

$$1,\ a,\ a^2,\ \ldots,\ a^{r-1} \tag{36}$$

są oczywiście różne oraz ciąg ten powtarza się cyklicznie w ciągu nieskończonym $1,\ a,\ a^2,\ \ldots,$ tzn.

$$a^m = a^n \Leftrightarrow m \equiv n \pmod{r}. \tag{37}$$

Rząd elementu możemy więc określić jako liczbę jego różnych potęg.

Głównym faktem, który teraz wykażemy, będzie istnienie w dowolnym ciele skończonym elementu, którego potęgi przebiegają wszystkie elementy niezerowe ciała. Doprowadzi nas do tego następująca seria prostych lematów.

LEMAT 16. *Jeśli a jest elementem rzędu r, to $a^m = 1$ wtedy i tylko wtedy, gdy m jest wielokrotnością r.*

Dowód. Wynika to bezpośrednio z (37), jeśli przyjmiemy $n = 0$. □

LEMAT 17. *Jeśli a jest elementem rzędu r, b elementem rzędu s, przy czym $(r, s) = 1$, to rząd elementu ab wynosi rs.*

Dowód. Należy wykazać, że $(ab)^k = 1$ wtedy i tylko wtedy, gdy k jest wielokrotnością rs. W tym celu załóżmy najpierw, że $(ab)^k = 1$. Mamy wtedy $a^k = b^{-k}$, $a^{rk} = b^{-rk} = 1$, $b^{-sk} = a^{sk} = 1$. Na mocy poprzedniego lematu $r|sk$. Lecz $(r, s) = 1$, zatem k jest wielokrotnością r. Podobnie, z równości $b^{-rk} = 1$ wnioskujemy, że k jest wielokrotnością s. Tak więc k jest wielokrotnością rs.

Na odwrót, jeśli k jest wielokrotnością rs, to oczywiście $(ab)^k = a^k b^k = 1$. □

LEMAT 18. *Jeśli a jest elementem rzędu r, to rząd elementu a^k wynosi $r/(r, k)$.*

Dowód. Oznaczmy przez s rząd elementu a^k. Mamy wtedy

$$(a^k)^{r/(r,k)} = (a^r)^{k/(r,k)} = 1^{k/(r,k)} = 1.$$

Z lematu 16 wnioskujemy, że

$$s \left| \frac{r}{(r, k)} \right. . \tag{38}$$

Z drugiej strony, wobec $1 = (a^k)^s = a^{ks}$, ks jest wielokrotnością r, a więc tym bardziej wielokrotnością $r/(r, k)$. Liczby $r/(r, k)$ i k są względnie pierwsze, zatem

$$\left. \frac{r}{(r, k)} \right| s. \tag{39}$$

Z (38) i (39) otrzymujemy natychmiast $s = r/(r, k)$, co kończy dowód. □

Elementem pierwotnym w ciele o q elementach nazywamy dowolny element rzędu $q-1$, tzn. element, którego potęgi przebiegają wszystkie elementy niezerowe ciała.

TWIERDZENIE 19. *Każde ciało skończone zawiera co najmniej jeden element pierwotny.*

Dowód. Oznaczmy przez r największy spośród rzędów elementu ciała i niech a będzie elementem rzędu r. Oczywiście

$$r \leqslant q-1, \tag{40}$$

jako że potęgi $1, a, a^2, \ldots, a^{r-1}$ stanowią r różnych elementów niezerowych ciała. Wystarczy teraz wykazać, że $q-1 \leqslant r$. W tym celu rozważmy dowolny element $b \neq 0$ i oznaczmy przez s jego rząd. Zgodnie z lematem 18 rząd elementu $b^{(r,s)}$ wynosi $s/(r, s)$. Lecz liczby r i $s/(r, s)$ są względnie pierwsze, zatem na mocy lematu 15 rząd elementu $ab^{(r,s)}$ wynosi $rs/(r, s)$. Widzimy stąd, że s musi być dzielnikiem r, gdyż w przeciwnym przypadku mielibyśmy $rs/(r, s) > r$, wbrew założeniu o maksymalności rzędu r. Skoro rząd dowolnego niezerowego elementu jest dzielnikiem r, to każdy element niezerowy spełnia równanie $x^r - 1 = 0$. Lecz na mocy lematu 9 równanie to ma co najwyżej r pierwiastków. Stąd $q-1 \leqslant r$, co w połączeniu z nierównością (40) daje żądaną równość $r = q-1$. □

W języku teorii grup moglibyśmy udowodnione twierdzenie wyrazić następująco: Grupa multyplikatywna dowolnego ciała skończonego jest cykliczna. Każdy element pierwotny jest jej generatorem. Przedstawienie elementów niezerowych ciała w postaci

$$a^0, a^1, a^2, \ldots, a^{q-2},$$

gdzie a jest elementem pierwotnym, ma wiele zalet przy badaniu struktury grupy multyplikatywnej ciała. Równość $a^r a^s = a^{r+s}$ ustala izomorfizm tej grupy z grupą (addytywną) reszt modulo $q-1$. Możemy również łatwo wyznaczyć rząd każdego elementu: na mocy lematu 18 rząd elementu a^k jest równy $(q-1)/(q-1, k)$. W szczególności, liczba wszystkich elementów rzędu $q-1$, tzn. wszystkich elementów pierwotnych, jest równa $\varphi(q-1)$, gdzie φ oznacza *funkcję Eulera* zdefiniowaną następująco: $\varphi(n)$ jest ilością liczb naturalnych $k \leqslant n$ względnie pierwszych z n (por. rozdział 2, § 5). Odnotujmy jeszcze dwa ważne fakty otrzymane w dowodzie twierdzenia 19:

WNIOSEK 20. *Rząd dowolnego elementu ciała o q elementach jest dzielnikiem $q-1$.* □

WNIOSEK 21. *Każdy element ciała o q elementach spełnia równanie*

$$x^q - x = 0.$$

Dowód. Rząd dowolnego elementu jest dzielnikiem $q-1$, zatem każdy element niezerowy ciała spełnia równanie $x^{q-1} - 1 = 0$. Zero spełnia równanie $x = 0$, tak więc dowolny element spełnia równanie $x(x^{q-1} - 1) = x^q - x = 0$. □

Wniosek ten możemy sformułować w nieco silniejszej postaci, z której będziemy jeszcze korzystali:

LEMAT 22. *Każdy element ciała o q elementach spełnia dla dowolnego $n \geqslant 0$ równanie*

$$x^{q^n} - x = 0.$$

Dowód. Stosujemy indukcję względem n. Dla $n = 0$ lemat jest oczywiście prawdziwy. Jeśli $x^{q^{n-1}} - x = 0$, to wobec wniosku 21 mamy $x^{q^n} = (x^{q^{n-1}})^q = x^q = x$. □

Zobaczmy teraz jakie są elementy pierwotne w konkretnym przykładzie ciała $GF(7)$. Zachodzą następujące relacje przystawania modulo 7:

$$\begin{array}{llllll}
2^1 \equiv 2, & 2^2 \equiv 4, & 2^3 \equiv 1, & & & \\
3^1 \equiv 3, & 3^2 \equiv 2, & 3^3 \equiv 6, & 3^4 \equiv 4, & 3^5 \equiv 5, & 3^6 \equiv 1, \\
4^1 \equiv 4, & 4^2 \equiv 2, & 4^3 \equiv 1, & & & \\
5^1 \equiv 5, & 5^2 \equiv 4, & 5^3 \equiv 6, & 5^4 \equiv 2, & 5^5 \equiv 3, & 5^6 \equiv 1, \\
6^1 \equiv 6, & 6^2 \equiv 1. & & & &
\end{array}$$

Tak więc rzędy elementów 1, 2, 3, 4, 5, 6 wynoszą odpowiednio 1, 3, 6, 3, 6, 2, co oznacza, że 3 i 5 są elementami pierwotnymi.

Zauważmy jeszcze, że jeśli $q-1$ jest liczbą pierwszą – tak jak na przykład w przypadku skonstruowanego już przez nas ciała rzędu $q = 4$ – to wszystkie elementy niezerowe oprócz jedynki (również jedynka, gdy $q = 2$) są elementami pierwotnymi. Wynika to bezpośrednio z wniosku 20.

Następnym ważnym faktem, który obecnie wykażemy będzie to, że każde dwa ciała rzędu p^m są izomorficzne. W tym celu udowodnimy najpierw kilka pomocniczych lematów.

LEMAT 23. *Dla dowolnego wielomianu*

$$P(x) = \sum_{i=0}^{r} a_i x^i$$

nad ciałem skończonym charakterystyki p i dowolnej liczby $n \geqslant 0$

$$[P(x)]^{p^n} = \sum_{i=0}^{r} a_i^{p^n} x^{ip^n}.$$

Dowód. Wykażemy najpierw, że dla dowolnych wielomianów Q, R nad ciałem charakterystyki p mamy

$$(Q+R)^p = Q^p + R^p. \tag{41}$$

Istotnie, zgodnie z wzorem dwumiennym mamy

$$(Q+R)^p = \sum_{i=0}^{p} \binom{p}{i} Q^i R^{p-i}.$$

Iloczyn liczby naturalnej $\binom{p}{i}$ przez Q^iR^{p-i} należy tu rozumieć jako sumę $\binom{p}{i}$ składników równych Q^iR^{p-i}. Lecz

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1\cdot 2\cdot\ldots\cdot i},$$

skąd bezpośrednio wynika, że $\binom{p}{i}$ jest wielokrotnością p dla $0 < i < p$. Dla tych wartości i suma $\binom{p}{i}$ identycznych składników jest oczywiście w ciele charakterystyki p równa zeru. Dowodzi to wzoru (41). Z kolei wykażemy, że dla dowolnego $n \geqslant 0$

$$(Q+R)^{p^n} = Q^{p^n} + R^{p^n}. \tag{42}$$

Stosujemy w tym celu indukcję względem n. Dla $n = 0$ wzór (42) jest oczywiście prawdziwy. Jeśli założymy

$$(Q+R)^{p^{n-1}} = Q^{p^{n-1}} + R^{p^{n-1}},$$

to stosując wzór (41) do wielomianów $Q^{p^{n-1}}$, $R^{p^{n-1}}$ otrzymujemy

$$(Q+R)^{p^n} = [(Q+R)^{p^{n-1}}]^p = (Q^{p^{n-1}} + R^{p^{n-1}})^p =$$
$$= (Q^{p^{n-1}})^p + (R^{p^{n-1}})^p = Q^{p^n} + R^{p^n}.$$

Równość (42) możemy łatwo uogólnić na dowolną liczbę składników:

$$(Q_0 + \ldots + Q_r)^{p^n} = Q_0^{p^n} + (Q_1 + \ldots + Q_r)^{p^n} = \ldots = Q_0^{p^n} + \ldots + Q_r^{p^n}.$$

Przyjmując $Q_i = a_i x^i$ otrzymujemy ostatecznie

$$\Big(\sum_{i=0}^{r} a_i x^i\Big)^{p^n} = \sum_{i=0}^{r} (a_i x^i)^{p^n} = \sum_{i=0}^{r} a_i^{p^n} x^{ip^n}. \quad \square$$

Jeśli współczynniki a_i są liczbami ciała, to zgodnie z lematem 22 mamy $a_i^{p^n} = a_i$, jako że liczby ciała charakterystyki p tworzą ciało o p elementach. Mamy wtedy

$$\sum_{i=0}^{r} a_i^{p^n} x^{ip^n} = \sum_{i=0}^{r} a_i (x^{p^n})^i.$$

Fakt ten możemy wyrazić następująco:

LEMAT 24. *Dla dowolnego wielomianu P nad ciałem $GF(p)$, gdzie p jest liczbą pierwszą, oraz dowolnej liczby $n \geqslant 0$*

$$[P(x)]^{p^n} = P(x^{p^n}). \quad \square$$

Wynika stąd następujące

Twierdzenie 25. *Jeśli P jest wielomianem nad podciałem prostym pewnego ciała skończonego F charakterystyki p oraz dla pewnego elementu* $a \in F$ *mamy* $P(a) = 0$, *wtedy dla dowolnego* $n \geqslant 1$

$$P(a^{p^n}) = 0.$$

Jeśli więc a jest pierwiastkiem wielomianu P, to

(43) $$a,\ a^p,\ a^{p^2},\ a^{p^3},\ \ldots$$

są też pierwiastkami wielomianu P. Oczywiście ciąg (43) zawiera tylko skończoną liczbę różnych elementów. Liczba ta zależy jednakże od rzędu r elementu a. Zauważmy, że zgodnie ze wzorem (37)

$$a^{p^i} = a^{p^j} \Leftrightarrow p^i \equiv p^j \pmod r.$$

Załóżmy, że $i < j$. Wtedy $p^i \equiv p^j \pmod r$ równoważne jest temu, że

(44) $$r | (p^{j-i} - 1)p^i.$$

Lecz jeśli rząd ciała F wynosi $q = p^m$, to na mocy wniosku 20 r dzieli $p^m - 1$, a stąd $(r, p) = 1$. Tak więc zamiast (44) możemy napisać

(45) $$p^{j-i} \equiv 1 \pmod r.$$

Jeśli oznaczymy przez s multyplikatywny rząd liczby p modulo r, tzn. najmniejszą liczbę $k > 0$ taką, że $p^k \equiv 1 \pmod r$, to wzór (45) jest równoważny temu, że $j - i$ jest wielokrotnością s. Ostatecznie więc

(46) $$a^{p^i} = a^{p^j} \Leftrightarrow j - i \equiv 0 \pmod s$$

i ciąg (43) zawiera dokładnie s różnych elementów $a,\ a^p,\ a^{p^2},\ \ldots,\ a^{p^{s-1}}$, które powtarzają się cyklicznie. Liczbę s nazywamy *stopniem* elementu a.

Twierdzenie 26. *Dla każdego elementu a ciała skończonego F charakterystyki p istnieje dokładnie jeden wielomian unormowany M nierozkładalny nad podciałem prostym ciała F taki, że* $M(a) = 0$. *Wielomian ten jest równy*

(47) $$M(x) = \prod_{i=0}^{s-1} (x - a^{p^i}),$$

gdzie s jest stopniem elementu a.

Dowód. Wykażemy najpierw, że współczynniki wielomianu M określonego wzorem (47) są liczbami ciała F. Niech $M(x) = \sum_{i=0}^{s} a_i x^i$. Obliczymy $[M(x)]^p$ dwoma sposobami. Z jednej strony, zgodnie z lematem 23,

(48) $$[M(x)]^p = \sum_{i=0}^{s} a_i^p x^{ip}.$$

Z drugiej strony,

(49)
$$[M(x)]^p = \prod_{i=0}^{s-1}(x-a^{p^i})^p = \prod_{i=0}^{s-1}(x^p - a^{p^{i+1}}) =$$
$$= \prod_{i=1}^{s}(x^p - a^{p^i}) = \prod_{i=0}^{s-1}(x^p - a^{p^i}) =$$
$$= M(x^p) = \sum_{i=0}^{s} a_i x^{ip}.$$

W powyższych przekształceniach korzystaliśmy z tego, że $(x-a^{p^i})^p = x^p - a^{p^{i+1}}$ – jest to wniosek z lematu 23, gdyż $(x+(-a^{p^i}))^p = x^p + (-a^{p^i})^p = x^p - a^{p^{i+1}}$ dla p nieparzystego, zaś $-a^{p^i} = a^{p^i}$ w ciele charakterystyki 2 – oraz z tego, że $a^{p^0} = a^{p^s}$ (p. wzór (46)). Porównując współczynniki wielomianu $[M(x)]^p$ we wzorach (48) i (49) widzimy, że $a_i^p = a_i$ dla $0 \leqslant i \leqslant s$. Ze wzoru (21) wynika, że każda spośród p liczb ciała charakterystyki p jest pierwiastkiem wielomianu $x^p - x$. Lecz wielomian ten jest stopnia p, zatem wobec lematu 9 liczby ciała są jego jedynymi pierwiastkami. Tak więc współczynniki a_i są liczbami ciała F.

Jeśli $M(x) = Q(x)R(x)$ dla pewnych wielomianów Q, R nad podciałem prostym ciała F, to jeden z wielomianów Q, R – na przykład Q – ma pierwiastek a. Lecz zgodnie z twierdzeniem 25 również a^p, a^{p^2}, ..., $a^{p^{s-1}}$ są pierwiastkami wielomianu Q. Wynika stąd, że M dzieli Q, czyli $\deg Q = \deg M$. Wykazaliśmy w ten sposób nierozkładalność wielomianu M.

Załóżmy teraz, że S jest unormowanym wielomianem nierozkładalnym nad podciałem prostym ciała F, takim, że $S(a) = 0$. Jak już zauważyliśmy, M dzieli wtedy S. Lecz S jest wielomianem nierozkładalnym, musi więc być $S = cM$ dla pewnego $c \in F$. Wielomiany S i M są unormowane, stąd $c = 1$, tzn. $S = M$. Dowód twierdzenia jest tym samym zakończony. □

Wielomian M określony wzorem (47) nazywamy *wielomianem minimalnym* elementu a. Jak widzimy, jego stopień jest równy stopniowi elementu a. Z twierdzenia 26 wynika bezpośrednio, że elementom a, a^p, a^{p^2}, ..., a^{p^s}, gdzie s jest stopniem a, odpowiada ten sam wielomian minimalny. Elementy te nazywamy *sprzężonymi*. Jest oczywiste, że jeśli jeden z tych elementów jest pierwiastkiem pewnego wielomianu nad podciałem prostym ciała F, to wszystkie one są jego pierwiastkami.

Na mocy wniosku 21 każdy element a ciała o p^m elementach spełnia równanie $a^{p^0} = a^{p^m}$. Zgodnie ze wzorem (46) mamy więc $m \equiv 0 \pmod{s}$, gdzie s jest stopniem elementu a. Daje to następujący lemat:

LEMAT 27. *W ciele rzędu p^m, gdzie p jest liczbą pierwszą, stopień każdego elementu jest dzielnikiem liczby m.* □

Do dowodu tego, że każde dwa ciała tego samego rzędu są izomorficzne potrzebny nam będzie jeszcze jeden lemat.

LEMAT 28. *Niech P będzie wielomianem nierozkładalnym stopnia n nad podciałem prostym ciała F o p^m elementach. Jeśli n dzieli m, to P ma w F dokładnie n pierwiastków, w przeciwnym przypadku P nie ma pierwiastków w F.*

Dowód. Wszystkie elementy ciała F możemy podzielić na podzbiory rozłączne odpowiadające zbiorom elementów sprzężonych. Na mocy twierdzenia 26 podzbiory te dają w sumie całe ciało F. Każdy taki podzbiór jest zbiorem pierwiastków pewnego jednoznacznie wyznaczonego unormowanego wielomianu nierozkładalnego nad podciałem prostym ciała F. Wobec lematu 27 stopień tego wielomianu jest dzielnikiem liczby m. Zgodnie z lematem 12

$$p^m = \sum_{n:\, n|m} nI_n.$$

Lewa strona tej równości wyraża liczbę elementów ciała F. Prawa strona wyrażałaby liczbę wszystkich pierwiastków wszystkich wielomianów unormowanych, stopni dzielących m, nierozkładalnych nad podciałem prostym ciała F, gdyby każdy taki wielomian stopnia $n|m$ miał w F dokładnie n pierwiastków. Każdy taki wielomian musi więc mieć rzeczywiście n pierwiastków w F — w przeciwnym przypadku dla pewnych elementów „zabrakłoby" wielomianów minimalnych.

Jeśli stopień wielomianu P nie dzieli m, to P nie może mieć pierwiastka w F, gdyż wielomian minimalny tego pierwiastka dzieliłby wielomian P, wbrew nierozkładalności. □

TWIERDZENIE 29. *Każde dwa ciała skończone tego samego rzędu są izomorficzne.*

Dowód. Niech rząd ciała F wynosi p^m, gdzie p jest liczbą pierwszą oraz $m \geqslant 1$. Z twierdzenia 5 wynika, że p jest charakterystyką ciała F. Podciało proste naszego ciała możemy więc utożsamiać z $GF(p)$. Ustalmy teraz pewien wielomian P stopnia m nierozkładalny nad $GF(p)$. Na mocy poprzedniego lematu istnieje element $a \in F$ taki, że $P(a) = 0$. Udowodnimy, że ciało F jest izomorficzne z ciałem reszt modulo P.

Wykażemy najpierw, że każdy element $b \in F$ daje się przedstawić jednoznacznie w postaci

$$b = \sum_{i=0}^{m-1} c_i a^i, \qquad c_i \in GF(p) \quad \text{dla } 0 \leqslant i \leqslant m-1. \tag{50}$$

W tym celu wystarczy zauważyć dwa fakty. Po pierwsze, wszystkich możliwych sum (50) jest p^m, gdyż każdy współczynnik c_i może przyjmować p wartości. Po drugie, każde dwie takie sumy dają różne elementy b. Istotnie, jeśli

$$b = \sum_{i=0}^{m-1} c_i' a^i,$$

to a jest pierwiastkiem wielomianu $\sum_{i=0}^{m-1}(c_i-c_i')x^i$ stopnia mniejszego od m, co na mocy twierdzenia 26 jest możliwe tylko wtedy, gdy $c_i' = c_i$ dla $0 \leqslant i \leqslant m-1$.

Aby obliczyć iloczyn dwu elementów postaci (50), wystarczy pomnożyć przez siebie odpowiadające im wielomiany. Wynik możemy oczywiście zredukować modulo wielomian $P(x)$ dla $x = a$, jako że $P(a) = 0$. Wykazaliśmy tym samym, że przyporządkowanie klasie wyznaczonej przez wielomian $\sum_{i=0}^{m-1} c_i x^i$ elementu $\sum_{i=0}^{m-1} c_i a^i$ ustala izomorfizm między ciałem utworzonym przez klasy reszt modulo P oraz ciałem F. Ciało F było dowolnym ciałem rzędu p^m, P zaś pewnym ustalonym wielomianem. Dowód twierdzenia jest tym samym zakończony. □

Jedyne z dokładnością do izomorfizmu ciało rzędu q będziemy oznaczali przez $GF(q)$ i nazywali *ciałem Galois rzędu q*. Definicja ta jest oczywiście rozszerzeniem podanej poprzednio definicji ciała Galois $GF(p)$, gdzie p jest liczbą pierwszą.

Zauważmy dla przykładu, że ciało rzędu 16 możemy reprezentować przez klasy reszt wielomianów nad $GF(2)$ modulo jeden z $\frac{1}{4}(2^4-2^2) = 3$ wielomianów stopnia czwartego nierozkładalnych nad $GF(2)$, bądź też przez klasy reszt wielomianów nad $GF(4)$ modulo jeden z $\frac{1}{2}(4^2-4) = 6$ wielomianów stopnia drugiego nierozkładalnych nad $GF(4)$. Na mocy twierdzenia 29 każda spośród tych dziewięciu reprezentacji określa to samo ciało, a mianowicie $GF(16)$.

Zajmiemy się teraz strukturą podciał w ciałach Galois.

TWIERDZENIE 30. *Ciało $GF(p^m)$ ma dla każdej liczby n dzielącej m dokładnie jedno podciało izomorficzne z $GF(p^n)$. Jest ono złożone ze wszystkich elementów ciała $GF(p^m)$ spełniających równanie*

$$x^{p^n} - x = 0. \tag{51}$$

Są to wszystkie podciała ciała $GF(p^m)$.

Dowód. Wykażemy najpierw, że zbiór elementów ciała $GF(p^m)$ spełniających równanie (51) tworzy podciało. Istotnie, jeśli $a^{p^n} = a$, $b^{p^n} = b$, to

$$(ab)^{p^n} = a^{p^n}b^{p^n} = ab,$$
$$(a+b)^{p^n} = a^{p^n}+b^{p^n} = a+b \quad \text{(na mocy lematu 23)},$$
$$(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1},$$
$$(-a)^{p^n} = -(a^{p^n}) = -a \quad \text{(jeśli } p^n \text{ parzyste, tzn. } p=2, \text{ to } a=-a).$$

Zauważmy teraz, że na mocy wzoru (46) równanie (51) jest spełnione przez dokładnie te elementy, których stopień dzieli n. Na mocy twierdzenia 26, lematu 28 i lematu 12 elementów takich jest

$$\sum_{s:\, s|n} sI_s = p^n.$$

Lecz wobec wniosku 21 każdy element ciała o p^n elementach spełnia równanie (51). Zbiór pierwiastków tego równania tworzy więc jedyne podciało rzędu p^n ciała $GF(p^m)$. Ostatnia część twierdzenia wynika bezpośrednio z twierdzenia 5. □

Wobec twierdzenia 30 będziemy zawsze traktowali $GF(p^n)$ jako podciało ciała $GF(p^m)$ dla $n|m$.

Podciało $GF(p^n)$ łatwo wyodrębnić z $GF(p^m)$, jeśli elementy niezerowe $GF(p^m)$ przedstawimy w postaci

$$a,\, a^2,\, a^3,\, \ldots,\, a^{p^m-1} = 1,$$

gdzie a jest pewnym elementem pierwotnym w $GF(p^m)$. Elementy niezerowe podciała $GF(p^n)$ spełniają równanie $x^{p^n-1} = 1$, są to zatem elementy a^k takie, że $k(p^n-1)$ jest wielokrotnością p^m-1. Lecz jeśli $n|m$, to p^n-1 dzieli p^m-1, gdyż dla dowolnego $m = dn+j$

(52) $$(p^{dn+j}-1) = p^j(p^n-1)(p^{(d-1)n}+p^{(d-2)n}+\ldots+p^n+1)+(p^j-1).$$

Jeśli oznaczymy

$$r = (p^m-1)/(p^n-1),$$

to $k(p^n-1)$ jest wielokrotnością p^m-1 wtedy i tylko wtedy, gdy k jest wielokrotnością r. Zatem elementy podciała $GF(p^n)$ możemy przedstawić w postaci

$$a^r,\, a^{2r},\, \ldots,\, a^{(p^n-1)r} = 1.$$

Zauważmy jeszcze, że dla dowolnego n, niekoniecznie dzielącego m, rząd elementu pierwotnego ciała $GF(p^n)$ wynosi p^n-1. Jeśli $GF(p^n)$ jest podciałem $GF(p^m)$, to wobec wniosku 20 p^n-1 dzieli p^m-1. Lecz ze wzoru (52) wynika, że jest to możliwe tylko wtedy, gdy $n|m$. Stanowi to niezależny dowód ostatniej części twierdzenia 30.

Jeśli a jest elementem pierwotnym w $GF(p^m)$, to elementy

$$a^{p^0},\, a^{p^1},\, \ldots,\, a^{p^{m-1}}$$

są różne, tzn. a jest stopnia m. Tak więc zgodnie z twierdzeniem 26 a jest pierwiastkiem pewnego wielomianu m-tego stopnia nierozkładalnego nad $GF(p)$. Do dowodu twierdzenia Singera (rozdział 7, twierdzenie 6.1) potrzebne nam będzie pewne uogólnienie tego faktu:

TWIERDZENIE 31. *Niech a będzie elementem pierwotnym ciała $GF(p^m)$ i niech $n|m$. Wtedy istnieje wielomian P stopnia $d = m/n$ nierozkładalny nad $GF(p^n)$ taki, że $P(a) = 0$.*

Dowód. Wielomian P określamy następująco:

(53) $$P(x) = \prod_{i=0}^{d-1} (x - a^{p^{in}}).$$

Załóżmy, że wielomian ten ma rozwinięcie $\sum_{i=0}^{d} a_i x^i$. Obliczymy na dwa sposoby $[P(x)]^{p^n}$. Z jednej strony, lemat 23 daje

$$[P(x)]^{p^n} = \sum_{i=0}^{d} a_i^{p^n} x^{ip^n}. \tag{54}$$

Z drugiej strony, w sposób analogiczny jak w dowodzie twierdzenia 26, wykazujemy, że

$$\begin{aligned}[P(x)]^{p^n} &= \prod_{i=0}^{d-1} (x - a^{p^{in}})^{p^n} = \prod_{i=0}^{d-1} (x^{p^n} - a^{p^{(i+1)n}}) = \\ &= \prod_{i=1}^{d} (x^{p^n} - a^{p^{in}}) = \prod_{i=0}^{d-1} (x^{p^n} - a^{p^{in}}) = \\ &= P(x^{p^n}) = \sum_{i=0}^{d} a_i x^{ip^n}.\end{aligned} \tag{55}$$

Z porównania (54) i (55) otrzymujemy $a_i^{p^n} = a_i$, co oznacza, na mocy twierdzenia 30, że $a_i \in GF(p^n)$.

Jeśli a jest pierwiastkiem pewnego wielomianu Q nad $GF(p^n)$, to z lematu 23 wynika, że $Q(x^{p^n}) = [Q(x)]^{p^n}$, a więc również $a^{p^n}, a^{p^{2n}}, \ldots, a^{p^{(d-1)n}}$ są pierwiastkami tego wielomianu, i w konsekwencji jest on podzielny przez P. Wynika stąd łatwo nierozkładalność wielomianu P nad $GF(p^n)$. □

Ogólnie, dla dowolnego a wielomian $P(x)$ określony wzorem (53), w którym d jest liczbą różnych elementów wśród $a, a^{p^n}, a^{p^{2n}}, \ldots$ — tzn. multyplikatywnym rzędem liczby p^n modulo rząd elementu a — nazywamy *wielomianem minimalnym* elementu a nad $GF(p^n)$.

W dowodzie twierdzenia 29 wykazaliśmy, że elementy ciała $GF(p^m)$ można przedstawiać jednoznacznie przez wielomiany $\sum_{i=0}^{m-1} c_i a^i$, gdzie a jest pierwiastkiem pewnego wielomianu stopnia m nierozkładalnego nad podziałem $GF(p)$. W identyczny sposób możemy udowodnić następujące uogólnienie tego faktu.

TWIERDZENIE 32. *Niech q będzie potęgą liczby pierwszej, zaś $n \geqslant 1$. Każdy element ciała $GF(q^n)$ możemy przedstawić jednoznacznie w postaci*

$$\sum_{i=1}^{n-1} c_i a^i, \qquad c_i \in GF(q) \quad \text{dla } 0 \leqslant i \leqslant m-1,$$

gdzie a jest pierwiastkiem pewnego wielomianu stopnia n nierozkładalnego nad podciałem $GF(q)$ ciała $GF(q^n)$. □

Zajmiemy się teraz strukturą grupy wszystkich automorfizmów ciała $GF(p^m)$.

TWIERDZENIE 33. *Grupa wszystkich automorfizmów ciała $GF(p^m)$ jest grupą cykliczną rzędu m generowaną przez automorfizm $\alpha\colon x \mapsto x^p$.*

Dowód. Wykażemy najpierw, że przekształcenie α: $x \mapsto x^p$ jest rzeczywiście automorfizmem. Tak jest w istocie, gdyż

$$\alpha(ab) = (ab)^p = a^p b^p = \alpha(a)\alpha(b),$$

$$\alpha(a+b) = (a+b)^p = a^p + b^p = \alpha(a) + \alpha(b)$$

(por. wzór (41)). Jeśli $a^p = b^p$, to

$$0 = a^p - b^p = a^p + (-b)^p = (a-b)^p,$$

czyli $a = b$.

Automorfizm α: $x \mapsto x^p$ generuje cykliczną grupę automorfizmów złożoną z

(56) $$\alpha, \alpha^2, \ldots, \alpha^m.$$

Zauważmy, że na mocy wniosku 21 automorfizm α^m: $x \mapsto x^{p^m}$ jest identycznością, tzn. jedynką tej grupy. Oczywiście, automorfizmy (56) są parami różne — przeprowadzają one element pierwotny (ogólniej, każdy element stopnia m) ciała $GF(p^m)$ na m różnych elementów.

Wystarczy teraz wykazać, że $GF(p^m)$ ma co najwyżej m różnych automorfizmów. W tym celu zauważmy najpierw, że dla dowolnego automorfizmu β mamy $\beta(1) = 1$, i w konsekwencji dla każdej liczby $c = \sum_{i=1}^{n} 1$ ciała $GF(p^m)$

$$\beta(c) = \beta\Big(\sum_{i=1}^{n} 1\Big) = \sum_{i=1}^{n} \beta(1) = \sum_{i=1}^{n} 1 = c.$$

Każdy automorfizm jest zatem stały na elementach podciała $GF(p)$.

Niech $P(x) = \sum_{i=0}^{m} f_i x^i$ będzie dowolnym wielomianem stopnia m nierozkładalnym nad $GF(p)$. Jak już zauważyliśmy w dowodzie twierdzenia 29, każdy element $b \in GF(p^m)$ daje się przedstawić jednoznacznie w postaci

$$b = \sum_{i=0}^{m-1} c_i a^i, \qquad c_i \in GF(p) \quad \text{dla } 0 \leqslant i \leqslant m-1$$

dla pewnego $a \in GF(p^m)$ takiego, że $P(a) = 0$ (taki element a istnieje na mocy lematu 28). Dla dowolnego automorfizmu β mamy

$$\beta(b) = \sum_{i=0}^{m-1} \beta(c_i)\beta(a^i) = \sum_{i=0}^{m-1} c_i\,[\beta(a)]^i.$$

Tak więc każdy automorfizm β jest jednoznacznie wyznaczony przez element $\beta(a)$. Lecz $\beta(a)$ musi być pierwiastkiem wielomianu P, gdyż

$$0 = \beta\big(P(a)\big) = \sum_{i=0}^{m} \beta(f_i)\beta(a^i) = \sum_{i=0}^{m} f_i\,[\beta(a)]^i = P\big(\beta(a)\big).$$

Wielomian P ma co najwyżej m pierwiastków, a więc $GF(p^m)$ nie może mieć więcej niż m automorfizmów. Zatem grupa cykliczna generowana przez α: $x \mapsto x^p$ jest grupą wszystkich automorfizmów ciała $GF(p^m)$. □

Na zakończenie zilustrujemy niektóre pojęcia dotyczące ciał skończonych na kilku przykładach.

Zaczniemy od ciała $GF(16)$. Możemy je reprezentować przez klasy reszt wielomianów nad $GF(2)$ modulo pewien wielomian P nierozkładalny nad $GF(2)$. Mamy do dyspozycji $I_4 = \frac{1}{4}(2^4 - 2^2) = 3$ takie wielomiany:

$$P_1(x) = x^4 + x^3 + x^2 + x + 1,$$

$$P_2(x) = x^4 + x^3 + 1,$$

$$P_3(x) = x^4 + x + 1.$$

Można to sprawdzić bezpośrednio generując najpierw wszystkie wielomiany nierozkładalne stopnia pierwszego, potem stopnia drugiego, stopnia trzeciego i czwartego, jako te, których nie da się otrzymać jako iloczyn uprzednio wygenerowanych wielomianów stopni mniejszych:

Wielomiany nierozkładalne stopnia pierwszego:

$$x, \; x+1.$$

Wielomiany rozkładalne stopnia drugiego:

$$xx = x^2,$$

$$(x+1)^2 = x^2 + 1,$$

$$(x+1)(x+1) = x^2 + 1.$$

Wielomiany nierozkładalne stopnia drugiego:

$$x^2 + x + 1.$$

Wielomiany rozkładalne stopnia trzeciego:

$$xxx = x^3,$$

$$(x+1)xx = x^3 + x^2,$$

$$(x+1)(x+1)x = x^3 + x,$$

$$(x+1)(x+1)(x+1) = x^3 + x^2 + x + 1,$$

$$(x^2+x+1)x = x^3 + x^2 + x,$$

$$(x^2+x+1)(x+1) = x^3 + 1.$$

Wielomiany nierozkładalne stopnia trzeciego:

$$x^3 + x^2 + 1,$$

$$x^3 + x + 1.$$

Wielomiany rozkładalne stopnia czwartego:

$$xxxx = x^4,$$
$$(x+1)xxx = x^4+x^3,$$
$$(x+1)(x+1)xx = x^4+x^2,$$
$$(x+1)(x+1)(x+1)x = x^4+x^3+x^2+x,$$
$$(x+1)(x+1)(x+1)(x+1) = x^4+1,$$
$$(x^2+x+1)xx = x^4+x^3+x^2,$$
$$(x^2+x+1)(x+1)x = x^4+x,$$
$$(x^2+x+1)(x+1)(x+1) = x^4+x^3+x+1,$$
$$(x^2+x+1)(x^2+x+1) = x^4+x^2+1,$$
$$(x^3+x^2+1)x = x^4+x^3+x,$$
$$(x^3+x^2+1)(x+1) = x^4+x^2+x+1,$$
$$(x^3+x+1)x = x^4+x^2+x,$$
$$(x^3+x+1)(x+1) = x^4+x^3+x^2+1.$$

Wielomiany nierozkładalne stopnia czwartego:

$$x^4+x^3+x^2+x+1,$$
$$x^4+x^3+1,$$
$$x^4+x+1.$$

x^k	$x^k \bmod (x^4+x^3+1)$	Rząd x^k	Wielomian minimalny
0	0		y
x^1	x	15	y^4+y^3+1
x^2	x^2	15	y^4+y^3+1
x^3	x^3	5	$y^4+y^3+y^2+y+1$
x^4	x^3+1	15	y^4+y^3+1
x^5	x^3+x+1	3	y^2+y+1
x^6	x^3+x^2+x+1	5	$y^4+y^3+y^2+y+1$
x^7	x^2+x+1	15	y^4+y+1
x^8	x^3+x^2+x	15	y^4+y^3+1
x^9	x^2+1	5	$y^4+y^3+y^2+y+1$
x^{10}	x^3+x	3	y^2+y+1
x^{11}	x^3+x^2+1	15	y^4+y+1
x^{12}	$x+1$	5	$y^4+y^3+y^2+y+1$
x^{13}	x^2+x	15	y^4+y+1
x^{14}	x^3+x^2	15	y^4+y+1
x^{15}	1	1	$y+1$

Przyjmijmy $P(x) = x^4+x^3+1$. Otrzymujemy wtedy reprezentację ciała $GF(16)$ przez wszystkie wielomiany stopni mniejszych niż cztery. Mnożenie elementów ciała odpowiada mnożeniu wielomianów, po którym następuje redukcja iloczynu modulo P. Element reprezentowany przez x okazuje się być jednym z elementów pierwotnych.

Rząd elementu x^k jest równy, jak wiemy, $15/(15, k)$. Mamy $\varphi(15) = 8$ elementów pierwotnych.

W $GF(2^4)$ mamy – oprócz samego $GF(2^4)$ – następujące podciała:

ciało $GF(2)$ złożone z elementów

$$0 \text{ i } x^{15} = 1,$$

ciało $GF(2^2)$ złożone z elementów

$$\begin{aligned} &0, \\ &x^5 = x^3+x+1, \\ &x^{10} = x^3+x, \\ &x^{15} = 1 \end{aligned}$$

(liczbę 5 otrzymujemy jako $(2^4-1)/(2^2-1)$).

W naszym przypadku element x jest oczywiście pierwiastkiem wielomianu $P(y) = y^4+y^3+1$. Wielomian ten jest również wielomianem minimalnym dla elementów $x^{2^1} = x^2$, $x^{2^2} = x^4$, $x^{2^3} = x^8$. Oczywiście każdy element pierwotny jest stopnia 4, lecz nie każdy element stopnia 4 jest elementem pierwotnym.

Zauważmy, że w naszym przykładzie pierwiastki sprzężone każdego z wielomianów minimalnych mają ten sam rząd. Nie jest to przypadek. Na mocy lematu 18 rząd elementu a^{p^i} ciała $GF(p^m)$ wynosi $r/(r, p^i)$, gdzie r jest rzędem elementu a. Lecz $r|(p^m-1)$, a stąd $(r, p^i) = 1$. Dla dowolnego $r|(p^m-1)$ możemy utworzyć iloczyn wszystkich wielomianów minimalnych, których pierwiastki mają rząd r. Iloczyn taki oznaczamy zwykle przez $Q^{(r)}$ i nazywamy *wielomianem kołowym rzędu r*. Jeśli r nie dzieli p^m-1, to przyjmujemy $Q^{(r)} = 1$. Ponieważ każdemu elementowi ciała odpowiada dokładnie jeden wielomian minimalny, zatem zbiór pierwiastków wielomianu $Q^{(r)}$ pokrywa się ze zbiorem elementów rzędu r, tzn.

(57) $$Q^{(r)}(y) = \prod_a (y-a),$$

gdzie a przebiega zbiór wszystkich elementów rzędu r. W naszym przykładzie

$$\begin{aligned} Q^{(1)}(y) &= y+1, \\ Q^{(3)}(y) &= y^2+y+1, \\ Q^{(5)}(y) &= y^4+y^3+y^2+y+1, \\ Q^{(15)}(y) &= (y^4+y^3+1)(y^4+y+1) = y^8+y^7+y^5+y^4+y^3+y+1. \end{aligned}$$

Iloczyn wszystkich wielomianów kołowych – równy oczywiście iloczynowi wszystkich unormowanych wielomianów nierozkładalnych nad $GF(p)$ – jest unormowanym wielomianem stopnia $p^m - 1$, zbiór pierwiastków którego pokrywa się ze zbiorem wszystkich niezerowych elementów ciała $GF(p^m)$. Tym wielomianem jest oczywiście $y^{p^m-1} - 1$ (p. wniosek 21). Tak więc

$$y^{p^m-1} - 1 = \prod_{r \mid p^m-1} Q^{(r)}(y).$$

Ogólnie, jeśli a jest elementem rzędu n dowolnego ciała, to elementy $1 = a^0$, a, $a^2, \ldots, a^{n-1}$ są pierwiastkami wielomianu $y^n - 1$. Lecz wielomian ten może mieć co najwyżej n pierwiastków. Stąd równość

$$y^n - 1 = \prod_{i=0}^{n-1} (y - a^i).$$

Zauważmy, że rząd dowolnego elementu a^i jest dzielnikiem n, dokładniej, jest równy $n/(n, i)$. Z drugiej strony, każdy element rzędu $r|n$ jest postaci a^i. Jest tak dlatego, iż każdy taki element jest pierwiastkiem wielomianu $y^r - 1$, a pierwiastki te to 1, $a^{n/r}$, $a^{2n/r}, \ldots, a^{(d-1)n/r}$. Możemy zatem napisać

$$y^n - 1 = \prod_{r:\, r|n} Q^{(r)}(y),$$

gdzie $Q^{(r)}(y)$ jest postaci (57). Używając multyplikatywnej wersji wzoru inwersyjnego Möbiusa (p. rozdział 2 wzór (2.15)) możemy stąd wyznaczyć wielomiany kołowe w jawnej postaci:

(58) $$Q^{(r)}(y) = \prod_{n:\, n|r} (y^n - 1)^{r/n}.$$

Najbardziej interesujące są dla nas zwykle wielomiany $Q^{(p^m-1)}(y)$, gdyż ich pierwiastki w $GF(p^m)$ pokrywają się z elementami pierwotnymi. Obliczmy dla przykładu $Q^{(15)}(y)$:

$$Q^{(15)}(y) = \frac{(y-1)(y^{15}-1)}{(y^3-1)(y^5-1)} = \frac{y^{10}+y^5+1}{y^2+y+1} = y^8 - y^7 + y^5 - y^4 + y^3 - y + 1.$$

W ciele charakterystyki 2 wielomian ten pokrywa się z uprzednio wyznaczonym wielomianem $y^8 + y^7 + y^5 + y^4 + y^3 + y + 1$.

Powróćmy do konstrukcji ciała $GF(16)$. Zauważmy, że jeśli wybierzemy $P_1(x) = x^4 + x^3 + x^2 + x + 1$ jako wielomian nierozkładalny w naszej konstrukcji, to element reprezentowany przez x nie byłby elementem pierwotnym. Mamy bowiem

$$x^5 \equiv 1 \pmod{x^4 + x^3 + x^2 + x + 1}.$$

Ciało $GF(16)$ możemy również skonstruować jako ciało reszt modulo pewien wielomian drugiego stopnia nierozkładalny nad $GF(4)$. Przedstawmy ciało $GF(4)$ jako ciało reszt modulo $S(z) = z^2+z+1$ nad $GF(2)$. Potrzebny nam będzie pewien wielomian stopnia drugiego nierozkładalny nad $GF(4)$.

Wielomiany (unormowane) stopnia pierwszego nierozkładalne nad $GF(4)$:

$$x,$$
$$x+1,$$
$$x+z,$$
$$x+(z+1).$$

Wielomiany stopnia drugiego rozkładalne nad $GF(4)$:

$$xx = x^2,$$
$$x(x+1) = x^2+x,$$
$$x(x+z) = x^2+zx,$$
$$x\big(x+(z+1)\big) = x^2+(z+1)x,$$
$$(x+1)(x+1) = x^2+1,$$
$$(x+1)(x+z) = x^2+(z+1)x+z,$$
$$(x+1)\big(x+(z+1)\big) = x^2+zx+(z+1),$$
$$(x+z)(x+z) = x^2+(z+1),$$
$$(x+z)\big(x+(z+1)\big) = x^2+x+1,$$
$$\big(x+(z+1)\big)\big(x+(z+1)\big) = x^2+z.$$

Wielomiany stopnia drugiego nierozkładalne nad $GF(4)$:

$$x^2+zx+1,$$
$$x^2+(z+1)x+1,$$
$$x^2+x+z,$$
$$x^2+zx+z,$$
$$x^2+x+(z+1),$$
$$x^2+(z+1)x+(z+1).$$

Wybierzmy pierwszy z tych wielomianów. Otrzymujemy wtedy następującą reprezentację ciała $GF(16)$, w której element zx jest elementem pierwotnym:

$(zx)^k$	$(zx)^k \pmod{x^2+zx+1}$	Rząd $(zx)^k$	Wielomian minimalny nad $GF(4)$
0	0		y
zx	zx	15	$y^2+(z+1)y+(z+1)$
$(zx)^2$	$x+(z+1)$	15	y^2+zy+z
$(zx)^3$	$zx+z$	5	$y^2+(z+1)y+1$
$(zx)^4$	$zx+(z+1)$	15	$y^2+(z+1)y+(z+1)$
$(zx)^5$	$(z+1)$	3	$y+(z+1)$
$(zx)^6$	x	5	y^2+zy+1
$(zx)^7$	$(z+1)x+z$	15	$y^2+y+(z+1)$
$(zx)^8$	$x+1$	15	y^2+zy+z
$(zx)^9$	$x+z$	5	y^2+zy+1
$(zx)^{10}$	z	3	$y+z$
$(zx)^{11}$	$(z+1)x$	15	y^2+y+z
$(zx)^{12}$	$zx+1$	5	$y^2+(z+1)y+1$
$(zx)^{13}$	$(z+1)x+(z+1)$	15	$y^2+y+(z+1)$
$(zx)^{14}$	$(z+1)x+1$	15	y^2+y+z
$(zx)^{15}$	1	1	$y+1$

Łatwo sprawdzić, że przyporządkowanie $(zx)^k \mapsto x^k$ ustala izomorfizm pomiędzy tą a poprzednią reprezentacją ciała $GF(16)$. Czasami wygodnie jest reprezentować wielomian $\sum_{i=0}^{m} a_i x^i$ przez m-kę $\langle a_m, a_{m-1}, \ldots, a_0\rangle$. Dla przykładu reprezentacja ciała $GF(3^3)$ przez reszty modulo x^3+2x+1 ma wtedy postać (x jest elementem pierwotnym):

0	$\langle 0, 0, 0\rangle$	x^{14}	$\langle 0, 2, 0\rangle$
x	$\langle 0, 1, 0\rangle$	x^{15}	$\langle 2, 0, 0\rangle$
x^2	$\langle 1, 0, 0\rangle$	x^{16}	$\langle 0, 2, 1\rangle$
x^3	$\langle 0, 1, 2\rangle$	x^{17}	$\langle 2, 1, 0\rangle$
x^4	$\langle 1, 2, 0\rangle$	x^{18}	$\langle 1, 2, 1\rangle$
x^5	$\langle 2, 1, 2\rangle$	x^{19}	$\langle 2, 2, 2\rangle$
x^6	$\langle 1, 1, 1\rangle$	x^{20}	$\langle 2, 1, 1\rangle$
x^7	$\langle 1, 2, 2\rangle$	x^{21}	$\langle 1, 0, 1\rangle$
x^8	$\langle 2, 0, 2\rangle$	x^{22}	$\langle 0, 2, 2\rangle$
x^9	$\langle 0, 1, 1\rangle$	x^{23}	$\langle 2, 2, 0\rangle$
x^{10}	$\langle 1, 1, 0\rangle$	x^{24}	$\langle 2, 2, 1\rangle$
x^{11}	$\langle 1, 1, 2\rangle$	x^{25}	$\langle 2, 0, 1\rangle$
x^{12}	$\langle 1, 0, 2\rangle$	x^{26}	$\langle 0, 0, 1\rangle$
x^{13}	$\langle 0, 0, 2\rangle$	$x^{27} = x$	$\langle 0, 1, 0\rangle$

Na zakończenie podamy pewne fakty dotyczące tzw. charakteru kwadratowego w ciałach Galois. *Charakter kwadratowy* w ciele $GF(p^m)$, gdzie p jest liczbą pierwszą nieparzystą, określamy jako funkcję χ: $GF(p^m) \to \{-1, 0, 1\}$ w następujący sposób:

$$\chi(a) = \begin{cases} 0, & \text{jeśli } a = 0, \\ 1, & \text{jeśli } a = b^2 \text{ dla pewnego } b \in GF(p^m) \setminus \{0\}, \\ -1, & \text{w pozostałych przypadkach.} \end{cases}$$

Mówimy, że a jest *kwadratem* lub *niekwadratem* w $GF(p^m)$ w zależności od tego, czy $\chi(a) = 1$, czy też $\chi(a) = -1$. W przypadku gdy $m = 1$, tzn. gdy $GF(p^m)$ jest ciałem reszt modulo p, używa się często – szczególnie w teorii liczb – symbolu Legendre'a zdefiniowanego następująco:

$$\left(\frac{x}{p}\right) = \chi(x \pmod p),$$

gdzie x jest dowolną liczbą całkowitą, χ zaś charakterem kwadratowym w $GF(p)$. Liczbę x nazywamy *resztą kwadratową modulo p*, jeśli $\left(\frac{x}{p}\right) = 1$ i *nieresztą kwadratową modulo p*, jeśli $\left(\frac{x}{p}\right) = -1$.

TWIERDZENIE 34. *Niech $q = p^m$, $m \geqslant 1$, gdzie p jest dowolną nieparzystą liczbą pierwszą, i niech χ będzie charakterem kwadratowym w $GF(q)$. Wtedy dla dowolnych $a, b \in GF(q)$ mamy*

(a) $\chi(a) = a^{(q-1)/2}$,

(b) $|\{a \in GF(q)\colon \chi(a) = 1\}| = |\{a \in GF(q)\colon \chi(a) = -1\}| = \frac{1}{2}(q-1)$,

(c) $\chi(ab) = \chi(a)\chi(b)$,

(d) $\chi(1) = 1$,

(e) $\chi(-1) = \begin{cases} 1, & \textit{jeśli } q \equiv 1 \pmod 4, \\ -1, & \textit{jeśli } q \equiv 3 \pmod 4, \end{cases}$

(f) $\chi(-a) = \begin{cases} \chi(a), & \textit{jeśli } q \equiv 1 \pmod 4, \\ -\chi(a), & \textit{jeśli } q \equiv 3 \pmod 4, \end{cases}$

(g) $\sum\limits_{y \in GF(q)} \chi(y)\chi(y+a) = \begin{cases} -1, & \textit{jeśli } a \neq 0, \\ q-1, & \textit{jeśli } a = 0. \end{cases}$

Dowód. (a) Załóżmy, że $a \neq 0$ – dla $a = 0$ wzór jest oczywiście prawdziwy – i oznaczmy $b = a^{(q-1)/2}$. Wobec wniosku 21 mamy $b^2 = a^{q-1} = 1$, czyli $b = 1$ lub $b = -1$, jako że wielomian $x^2 - 1$ nie może mieć więcej niż dwa pierwiastki (por. lemat 9). Jeśli a jest kwadratem, powiedzmy $a = c^2$, to $b = a^{(q-1)/2} = c^{q-1} = 1$, co dowodzi prawdziwości naszego wzoru dla przypadku, gdy a jest kwadratem. Równanie $x^{(q-1)/2} = 1$ ma co najwyżej $\frac{1}{2}(q-1)$ pierwiastków. Z drugiej strony, każda spośród $\frac{1}{2}(q-1)$ parzystych potęg ustalonego elementu pierwotnego jest kwadratem, a więc spełnia to równanie.

Wnioskujemy stąd, że jest dokładnie $\frac{1}{2}(q-1)$ kwadratów, i w konsekwencji $a^{(q-1)/2} = -1$, jeśli a jest niekwadratem, co kończy dowód wzoru (a). Przy okazji udowodniliśmy również (b). (c) i (d) są bezpośrednimi wnioskami z (a). Również (e) łatwo wynika z (a), gdyż $\frac{1}{2}(q-1)$ jest parzyste dla $q \equiv 1 \pmod 4$ i nieparzyste dla $q \equiv 3 \pmod 4$. (f) wynika bezpośrednio z (e) i (c). (g) Dla $a = 0$ wzór jest oczywisty, załóżmy więc, że $a \neq 0$. Dla każdego $y \neq 0$ rozważmy element $z = (y+a)/y$. Mamy $y+a = zy$, przy czym jeśli y przebiega wszystkie elementy niezerowe ciała $GF(q)$, to z przebiega wszystkie elementy różne od jedności. Wynika to z oczywistego faktu, iż $(y'+a)/y' = (y+a)/y$ tylko wtedy, gdy $y' = y$. Stąd

$$\sum_{y \in GF(q)} \chi(y)\chi(y+a) = \sum_{y \neq 0} \chi(y)\chi(y+a) =$$

$$= \sum_{y \neq 0} \chi(y)\chi(y)\chi\left(\frac{y+a}{y}\right) = \sum_{z \neq 1} \chi(z) = \sum_{z \in GF(q)} \chi(z) - \chi(1) = -1. \quad \square$$

Zadania

1. Wykazać, że ciało liczb zespolonych można otrzymać ze zbioru wielomianów nad ciałem liczb rzeczywistych utożsamiając wielomiany przystające modulo x^2+1. Czy istnieją wielomiany nierozkładalne nad ciałem liczb rzeczywistych stopnia większego od dwóch?

2. Udowodnić, że dla $m \geqslant 0$ liczba unormowanych wielomianów stopnia m nad ciałem skończonym F będących iloczynem nieparzystej liczby różnych czynników nierozkładalnych stopni niezerowych jest równa liczbie unormowanych wielomianów stopnia m nad F będących iloczynem parzystej liczby różnych czynników nierozkładalnych stopni niezerowych.

Wskazówka: Skorzystać ze wzoru (33).

3. Udowodnić, że dla dowolnego $r \geqslant 1$

$$\deg Q^{(r)} = \varphi(r),$$

gdzie φ jest funkcją Eulera.

4. Udowodnić, że nad dowolnym ciałem

$$(x^m - 1,\ x^n - 1) = x^{(m,n)} - 1.$$

5 (Wedderburn). Udowodnić, że jeśli F jest zbiorem skończonym, to przemienność mnożenia wynika z pozostałych aksjomatów ciała.

BIBLIOGRAFIA

Abbott, H. L., Hanson, D.
[1] *A problem of Schur and its generalizations*, Acta Arith. 20 (1972), str. 175–187.

Abbott, H. L., Liu, A. C.
[1] *On partitioning integers into progression free sets*, J. Combin. Theory 13 (1972), str. 432–436.
[2] *Remarks on a paper of Hirschfeld concerning Ramsey numbers*, Discrete Math. 39 (1982), str. 327–328.

Aho, A. V., Hopcroft, J. E., Ullman, J. D.
[1] *The design and analysis of computer algorithms*, Addison-Wesley, Reading, MA, 1974.

Aigner, M.
[1] *Combinatorial theory*, Springer-Verlag, Berlin 1979.

Ajtai, M., Komlós, J., Szemerédi, E.
[1] *A note on Ramsey numbers*, J. Combin. Theory, Ser. A 29 (1980), str. 354–360.

Alladi, K., Erdős, P., Hoggatt, V. E.
[1] *On additive partitions of integers*, Discrete Math. 22 (1978), str. 201–211.

Andrews, G. E.
[1] *On the foundations of combinatorial theory V: Eulerian differential operators*, Studies in Appl. Math. 50 (1971), str. 345–375.

Banach, S.
[1] *Un théorème sur les transformations biunivoques*, Fund. Math. 6 (1924), str. 236–239.

Banachowski, L., Kreczmar, A.
[1] *Elementy analizy algorytmów*, WNT, Warszawa 1984.

Baumert, L. D.
[1] *Cyclic difference sets*, Springer-Verlag, Berlin 1971.

Baumgartner, J. E.
[1] *A short proof of Hindman's theorem*, J. Combin. Theory, Ser. A 17 (1974), str. 384–386.

Beeler, M. D., O'Neil, P. E.
[1] *Some new van der Waerden numbers*, Discrete Math. 28 (1979), str. 135–146.

Bender, E. A., Goldman, J. R.
[1] *On the applications of Möbius inversion in combinatorial analysis*, Amer. Math. Monthly 82 (1975), str. 789–803.

Berge, C., Chvátal, V.
[1] *Topics on perfect graphs*, Ann. Discrete Math. 21 (1984).

Berlekamp, E. R.
[1] *A construction for partitions which avoid long arithmetic progressions*, Canad. Math. Bull. 11 (1968), str. 409–414.

Białynicki-Birula, A. S.
[1] *Algebra*, PWN, Warszawa 1971.

Birkhoff, G.
[1] *Tres observaciones sobre el algebra lineal*, Univ. Nac. Tucuman Rev. Ser. A5 (1946), str. 147–151.

de Bruijn, N. G.
[1] *Generalization of Pólya's fundamental theorem in enumeration combinatorial analysis*, Indag. Math. 21 (1959), str. 59–69.

de Bruijn, N. G., Erdös, P.
[1] *On a combinatorial problem*, Indag. Math. 10 (1948), str. 421–423.

Bose, R. C.
[1] *On the construction of balanced incomplete block designs*, Ann. Eugenics 9 (1939), str. 353–399.

Bose, R. C., Ray-Chaudhuri, D. K.
[1] *On a class of error correcting codes*, Inform. and Control 3 (1960), str. 68–79.

Bose, R. C., Shrikhande, S.
[1] *On the construction of sets of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Trans. Amer. Math. Soc. 95 (1960), str. 191–209.

Bose, R. C., Shrikhande, S., Parker, E. T.
[1] *Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture*, Canad. J. Math. 12 (1960), str. 189–203.

Bridges, W. G.
[1] *Some results on λ-designs*, J. Combin. Theory 8 (1970), str. 350–360.
[2] *A characterization of type-*1 *λ-designs*, J. Combin. Theory, Ser. A 22 (1977), str. 361–367.

Bridges, W. G., Kramer, E. S.
[1] *The determination of all λ-designs with $\lambda = 3$*, J. Combin. Theory 8 (1970), str. 343–349.

Brown, T. C.
[1] *Common transversals*, J. Combinatorial Theory 21 (1976), str. 80–85.
[2] *Common transvelsals for partitions of a finite set*, Discrete Math. 51 (1984), str. 119–124.

Burnside, W.
[1] *Theory of groups of finite order* (2nd edition), Cambridge Univ. Press, London 1911. Przedruk: Dover, New York 1955.

Burr,
[1] *Generalized Ramsey theory for graphs — a survey*, w: *Graphs and Combinatorics*, Springer-Verlag, 1974, str. 52–75.

Bruck, R. H., Ryser, H. J.
[1] *The nonexistence of certain finite projective planes*, Canad. J. Math. 1 (1949), str. 88–93.

Canfield, R.
[1] *On a problem of Rota*, Bull. Amer. Math. Soc. 84 (1978), str. 164.

Chowla S., Herstein, I.N., Scott, W. R.
[1] *The solutions of $x^d = 1$ in symmetric groups*. Norske Vid. Selsk. Forh. (Trondheim) 25 (1952), str. 29–31.

Chowla, S., Ryser, H. J.
[1] *Combinatorial problems*, Canad. J. Math. 2 (1950), str. 93–99.

Chung, F. R. K.
[1] *A note on constructive methods for Ramsey numbers*, J. Graph Theory 5 (1981), str. 109–113.

Clos, C.
[1] *A study of non-blocking switching networks*, Bell System Tech. J. 32 (1953), str. 406–424.

Crapo, H. H., Rota, G.-C.
[1] *On the foundations of combinatorial theory II: Combinatorial geometries*, MIT Press, Cambridge, MA, 1970.

Damerell, M. R., Milner, E. S.
[1] *Necessary and sufficient conditions for transversals of countable set systems*, J. Combinatorial Theory 17 (1974), str. 350–374.

Davis, R. L.
[1] *The number of structures of finite relations*, Proc. Amer. Math. Soc. 4 (1953), str. 486–495.

Dembowski, P.
[1] *Finite geometries*, Springer-Verlag, Berlin 1968.

Dénes, J., Keedwell, A. D.
[1] *Latin squares and their applications*, Akadémiai Kiadó, Budapest 1974.

Deuber, W.
[1] *Partitionen und lineare Gleichungssysteme*, Math. Z. 133 (1973), str. 109–123.
[2] *Generalizations of Ramsey's theorem*, w: *Infinite and finite sets*, Coll. Math. Soc. J. Bolyai 10 (1974), str. 323–332.
[3] *On van der Waerden's theorem on arithmetic progressions*, J. Combin. Theory, Ser. A, 32 (1982), str. 115–118.

Dilworth, R. P.
[1] *A decomposition theorem for partially ordered sets*, Ann. Math. 51 (1950), str. 161–166.
[2] *Some combinatorial problems on partially ordered sets*, w: *Combinatorial analysis*, Proc. Symp. Appl. Math., vol. X, Amer. Math. Soc., Providence, RI, 1960, str. 85–90.

Dobinski, G.
[1] Grunert's Archiv 61 (1877), str. 333–336.

Doubilet, P., Rota, G. C., Stanley, R. P.
[1] *On the foundations of combinatorial theory VI: The idea of generating function*, Proc. 6th Berkeley Symp. on Math. Stat. and Prob., vol. II: *Probability theory*, Univ. of California 1972, str. 267–318.

Duguid, A. M.
[1] *Structural properties of switching networks*, Techn. Rep. BTL 7, Brown University, Providence, RI, 1959.

Edmonds, J., Fulkerson, D. R.
[1] *Transversals and matroid partition*, J. Res. Nat. Bur. Standards 69B (1965), str. 147–153.

Egerváry, E.
[1] *Matrixok kombinatorius tulajdonsàgairol*, Mat. Fiz. Lapok 38 (1931), str. 16–28.

Erdös, P.
[1] *On a lemma of Littlewood and Offord*, Bull. Amer. Math. Soc. 51 (1945), str. 898.
[2] *Some remarks on the theory of graphs*, Bull Amer. Math. Soc. 53 (1947), str. 292–294.

Erdös P., Hajnal, Máté, A., Rado, R.
[1] *Combinatorial set theory: partition relations for cardinals*, North-Holland, Amsterdam, and Akadémiai Kiadó, Budapest 1984.

Erdös, P., Kleitman, D.
[1] *Extremal problems among subsets of a set*, Discrete Math. 8. (1974), str. 281–294.

Erdös, P., Ko, C., Rado, R.
[1] *Intersection theorems for systems of finite sets*, Quart. J. Math. Oxford Ser. (2) 12 (1961), str. 313–318.

Erdös, P., O'Neil, P. E.
[1] *On a generalization of Ramsey numbers*, Discrete Math. (1973), str. 29–35.

Erdös, P., Rado, R.
[1] *Combinatorial theorems on classifications of subsets of a given set*, Proc. London Math. Soc. 2 (1952), str. 417–439.

Erdős, P., Spencer, J.
[1] *Probabilistic methods in combinatorics*, Akadémiai Kiadó, Budapest 1974.

Erdős, P., Szekeres, G.
[1] *A combinatorial problem in geometry*, Compositio Math. 2 (1939), str. 463–470.

Fisher, R. A.
[1] *An examination of the different possible solutions of a problem of incomplete blocks*, Ann. Eugenics 10 (1940), str. 52–75.
[2] *The design of experiments*, Oliver and Boyd, Edinburgh 1935.

Flachsmayer, J.
[1] *Kombinatoryka*, PWN, Warszawa 1974.

Foata, D.
[1] *La série génératrice exponentielle dans les problèmes d'énumération*, Le Presse de l'Université de Montréal, Montréal 1974.

Ford, L. R., Fulkerson, D. R.
[1] *Flows in networks*, Princeton University Press, Princeton, NJ 1962. Polski przekład: *Przepływy w sieciach*, PWN, Warszawa 1969.

Frankl, P.
[1] *A probabilistic proof for the LYM-inequality*, Discrete Math. 43 (1983), str. 325.

Franklin, F.
[1] *Sur le développement du produit infini* $(1-x)(1-x^2)\ldots$, C. R. Acad. Sci. Paris 32 (1981), str. 448–450.

Fredricksen, H.
[1] *Schur numbers and the Ramsey numbers* $N(3, 3, \ldots, 3; 2)$, J. Combin. Theory, Ser. A 27 (1979), str. 376–377.

Frobenius, G.
[1] *Über Matrizen aus nicht negativen Elementen*, Sitzungsber. Preuss. Akad. Wiss. (1912), str. 456–477.

Frucht, R., Rota, G.-C.
[1] *La funcion de Möbius para particiones de un conjunto*, Scientia 122 (1963), str. 111–115.

Gerencsér, L., Gyárfás, A.
[1] *On Ramsey-type problems*, Ann. Univ. Sci. Budapest, Eötvös Sect. Mat. 10 (1967), str. 167–170.

Goldman, J. R., Rota, G.-C.
[1] *On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions*, Studies in Applied Math. 49 (1970), str. 239–258.

Golumbic, M. C.
[1] *Algorithmic graph theory and perfect graphs*, Academic Press, New York 1980.

Gottschalk, W. H.
[1] *Choice functions and Tychonoff's theorem*, Proc. Amer. Math. Soc. 2 (1951), str. 172.

Graham, R. L.
[1] *Maximum antichains in the partition lattice*, Math. Intelligencer 1 (1978), str. 84–86.

Graham, R. L., Leeb, K., Rothschild, B. L.
[1] *Ramsey's theorem for a class of categories*, Advances in Math. 8 (1972), str. 417–433, (Errata: 10 (1973), str. 326–327).

Graham, R. L., Rothschild, B. L.
[1] *Ramsey's theorem for n-parameter sets*, Trans. Amer. Math. Soc. 159 (1971), str 257–292.
[2] *A short proof of van der Waerden's theorem on arithmetic progressions*, Proc. Amer. Math. Soc. 42 (1974), str. 385–386.
[3] *Ramsey's theorem for n-dimensional arrays*, Bull. Amer. Math. Soc. 75 (1969), str. 418–422.

[4] *A survey of finite Ramsey theorems*, Proc. 2nd Louisiana Conf. on Combinatorics, Graph Theory and Computing, 1971, str. 21–40.

Graham, R. L., Spencer, J. H.
[1] *A general Ramsey product theorem*, Proc. Amer. Math. Soc. 73 (1979), str. 137–139.

Graver, J. E., Watkins, M. E.
[1] *Combinatorics with emphasis on the theory of graphs*, Springer-Verlag, New York, NY, 1977.

Greene, C., Kleitman, D.
[1] *Strong versions of Sperner's theorem*, J. Combin. Theory, Ser. A. 20 (1976), str. 80–88.

Griggs, J. R.
[1] *An upper bound on the Ramsey numbers $R(3, k)$*, J. Combin. Theory, Ser. A 35 (1983), str. 145–153.

Hales, A. W., Jewett, R. I.
[1] *Regularity and positional games*, Trans. Amer. Math. Soc. 106 (1963), str. 222–229.

Hall, M., Jr.
[1] *An existence theorem for Latin squares*, Bull. Amer. Math. Soc. 2 (1945), str. 387–388.
[2] *Distinct representatives of subsets*, Bull. Amer. Mat. Soc. 54 (1948), str. 922–926.
[3] *Combinatorial theory*, Blaisdell Publ. Co., Waltham, MA, 1967.

Hall, M., Ryser, H. J.
[1] *Cyclic incidence matrices*, Canad. J. Math. 3 (1951), str. 495–502.

Hall, P.
[1] *On representatives of subsets*, J. London Math. Soc. 10 (1935), str. 26–30.
[2] *The Eulerian functions of a group*, Quart. J. Math. Oxford Ser. 7 (1936), str. 134–151.

Hanani, H.
[1] *The existence and construction of balanced incomplete block designs*, Ann. Math. Statist. 32 (1961), str. 361–386.
[2] *On the number of orthogonal Latin squares*, J. Combin. Theory 8 (1970), str. 247–271.
[3] *On balanced incomplete block designs with blocks having five elements*, J. Combin. Theory 12 (1972), str. 184–201.
[4] *Balanced incomplete block designs and related designs*, Discrete Math. 11 (1975), str. 255–369.

Harary, F.
[1] *Recent results on generalized Ramsey theory for graphs*, Graph Theory and Applications (Y. Alavi, D. R. Lick, A. T. White, eds.), Lecture Notes in Math., vol. 303, Springer-Verlag, Berlin, 1972, str. 125–138.

Harary, F., Palmer, E. M.
[1] *Graphical enumeration*, Addison-Wesley, Reading, MA, 1973.

Harper, L. H., Rota, G.-C.
[1] *Matching theory: an introduction*, Advances in Probability 1 (1971), str. 169–213.

Harris, B., Schoenfeld
[1] *The number of idempotent elements in symmetric semigroups*, J. Combin. Theory 3 (1967), str. 122–135.

Hindman, N.
[1] *Finite sums from sequences within cells of a partition of N*, J. Combin. Theory 17 (1974), str. 1–11.

Hocquenghem, A.
[1] *Codes correcteurs d'erreurs*, Chiffres 2 (1959), str. 147–156.

Hopcroft, J., Karp, R. M.
[1] *An $n^{5/2}$ algorithm for maximum matchings in bipartite graphs*, SIAM J. Comput. 2 (1973), str. 225–231.

Huszár, G.

[1] *A kínai matematika történetének egy problémájáról*, Mat. Lapok 6 (1955), str. 36–38.

Kaplansky, I.

[1] *Solution of the "problème des ménages"*, Bull. Amer. Math. Soc. 49 (1943), str. 784–785.

Katona, G.

[1] *A simple proof of the Erdős–Ko–Rado theorem*, J. Combin. Theory Ser. B 13 (1972), str. 183–184.

Kaucký, J.

[1] *Kombinatorické identity*, Věda, Bratislava 1975.

Kirkman, T.

[1] *On a problem in combinatorics*, Cambridge and Dublin Math. J. 2 (1847), str. 191–204.

König, D.

[1] *Über eine Schlussweise aus dem Endlichen ins Unendliche*, Acta Litt. Ac. Sc. Univ. Hung. Franc. Josephinae, Sectio Sc. Math. 3 (1927), str. 121–130.

[2] *Graphok és matrixok*, Mat. Fiz. Lapok 38 (1931), str. 116–119.

[3] *Theorie der endlichen und unendlichen Graphen*, Leipzig 1936.

Kramer, E. S.

[1] *On λ-designs*, J. Combinatorial Theory 16 (1974), str. 57–75.

Kreid, T.

[1] *Kombinatoryczne ciągi wielomianów*, Rozprawa doktorska, Warszawa 1980.

Kuratowski, K.

[1] *Rachunek różniczkowy i całkowy, Funkcje jednej zmiennej*, wyd. V, PWN, Warszawa 1971.

Kuratowski, K., Mostowski, A.

[1] *Teoria mnogości*, PWN, Warszawa 1978.

Lah, I.

[1] *Eine neue Art von Zahlen, ihre Eigenschaften und Anwendung in der mathematischen Statistik*, Mitteilungsblatt Math. Stat. 7 (1955), str. 203–212.

Lipski, W.

[1] *Kombinatoryka dla programistów*, WNT, Warszawa 1982.

Lipski, W., Preparata, F. P.

[1] *Yet another permutation sequence*, Techn. Rep. ACT-10, Coordinated Science Lab., Univ. of Illinois, October 1978.

Lovász, L.

[1] *Normal hypergraps and the perfect graph conjecture*, Discrete Math. 2 (1972), str. 253–267.

[2] *A characterization of perfect graphs*, J. Combin. Theory Ser. B 13 (1972), str. 95–98.

[3] *Combinatorial problems and exercises*, Akadémiai Kiadó, Budapest 1979.

Longyear, J. Q.

[1] *Common transversals in partitioning families*, Discrete Math. 17 (1977), str. 327–329.

Lubell, D.

[1] *A short proof of Sperner's theorem*, J. Combin. Theory 1 (1966), str. 299.

MacMahon, P. A.

[1] *Combinatory analysis*, Cambridge Univ. Press, London 1915.

MacNeish, H. P.

[1] *Euler squares*, Ann. Math. 23 (1922), str. 221–227.

MacWilliams, F. J., Sloane, N. J. A.

[1] *The theory of error-correcting codes*, North-Holland, Amsterdam 1977.

Majumdar, K. N.
[1] *On some theorems in combinatorics relating to incomplete block designs*, Ann. Math. Statist. 24 (1953), str. 377–389.

Marek, W., Onyszkiewicz, J.
[1] *Elementy logiki i teorii mnogości w zadaniach*, wyd. 2, PWN, Warszawa 1975.

Menger, K.
[1] *Zur allgemeinen Kurventheorie*, Fund. Math. 10 (1927), str. 96–115.

Meshalkin, L. D.
[1] *A generalization of Sperner's theorem on the number of subsets of a finite set*, Theory Probability Appl. 8 (1963), str. 203–204.

Mills, G.
[1] *A quintessential proof of van der Waerden's theorem on arithmetic progressions*, Discrete Math. 47 (1983), str. 117–130.
[2] *Ramsey–Paris–Harrington numbers for graphs*, J. Combin. Theory, Ser. A 38 (1985), str. 30–37.

Mirsky, L.
[1] *Transversal theory*, Academic Press, New York 1971.

Mirsky, L., Perfect, H.
[1] *Applications of the notion of independence to problems of combinatorial analysis*, J. Combin. Theory 2 (1967), str. 327–357.

Moon, J.
[1] *Topics on tournaments*, Holt, New York 1968.

Moser, L.
[1] *On a theorem of van der Waerden*, Canad. Math. Bull. 3 (1960), str. 23–25.

Mostowski, A., Stark, M.
[1] *Elementy algebry wyższej*, wyd. 3 poprawione, PWN, Warszawa 1965.

Mullin, R. C., Nemeth, E.
[1] *An existence theorem for Room squares*, Canad. Math. Bull. 12 (1969), str. 493-497.

Mullin, R., Rota, G. C.
[1] *On the foundations of combinatorial theory III: Theory of binomial enumeration*, w: *Graph theory and its applications*, str. 167–213, Academic Press, New York 1970.

Nagell, T.
[1] *Introduction to number theory*, J. Wiley, New York, 1951.

Nara, C., Tachibana, S.
[1] *A note on upper bounds for some Ramsey numbers*, Discrete Math. 45 (1983), str. 323–326.

Nešetřil, J., Rödl, V.
[1] *The Ramsey property for graphs with forbidden complete subgraphs*, J. Combin. Theory 20 (1976), str. 243–249.
[2] *Another proof of the Folkman–Rado–Sanders theorem*, J. Combin. Theory, Ser. A 34 (1983), str. 108–109.

Niven, I.
[1] *Formal power series*, Amer. Math. Monthly 76 (1969), str. 871–889.

Ore, O.
[1] *Graphs and matching theorems*, Duke Math. J. 22 (1955), str. 625–639.

Paris, J., Harrington, L.
[1] *An incompleteness in Peano arithmetics*, w: J. Barwise (ed.), *Handbook of mathematical logic*, North–Holland, Amsterdam 1976.

Parker, E. T., Mood, A. N.
[1] *Some balanced Howell rotations for duplicate bridge sessions*, Amer. Math. Monthly 62 (1955), str. 714–716.

Peltesohn, R.
[1] *Eine Lösung der beiden Heffterschen Differenzenprobleme*, Compositio Math. 6 (1939), str. 251–257.

Peřfect, H.
[1] *Remark on a criterion for common transversals*, Glasgow Math. J. 10 (1969), str. 66–67.

Pólya, G.
[1] *Kombinatorische Anzahlbestimmung für Gruppen, Graphen und chemische Verbindungen*, Acta Math. 68 (1937), str. 145–254.

Rado, R.
[1] *Bemerkungen zur Kombinatorik im Anschluss an Untersuchungen von Herrn D. König*, Sitzungsber. Berliner Math. Gesellschaft 32 (1933), str. 60–75.
[2] *Studien zur Kombinatorik*, Math. Z. 36 (1933), str. 424–480.
[3] *Note on combinatorial analysis*, Proc. London Math. Soc. 48 (1943), str. 122–160.
[4] *Axiomatic treatment of rank in infinite sets*, Canad. J. Math. 1 (1949), str. 337–343.
[5] *Some partition theorems*, Colloq. Math. Soc. Janos Bolyai 4, P. Erdős, A. Renyi and V. Sos (eds.), *Combinatorial theory and its applications III*, North–Holland, Amsterdam 1970, str. 929–936.

Ramsey, F. P.
[1] *On a problem of formal logic*, Proc. London Math. Soc. 30 (1930), str. 264–286.

Ray-Chaudhuri, D. K., Wilson, R. M.
[1] *Solution of Kirkman's schoolgirl problem*, Proc. Symp. Pure Math., vol. XIX, Amer. Math. Soc., Providence, RI, 1971, str. 187–203.

Rasiowa, H.
[1] *Wstęp do matematyki współczesnej*, PWN, Warszawa 1968.

Rasiowa, H., Sikorski, R.
[1] *The mathematics of metamathematics*, PWN, Warszawa 1970.

Redfield, J. H.
[1] *The theory of group-reduced distributions*, Amer. J. Math. 49 (1927), str. 433–455.

Reiss, M.
[1] *Über eine Steinersche kombinatorische Aufgabe welche in 45sten Bande dieses Journals, Seite 181, gestellt worden ist*, J. Reine Angew. Math. 56 (1859), str. 326–344.

Riordan, J.
[1] *An introduction to combinatorial mathematics*, John Wiley and Sons, New York 1958.
[2] *Combinatorial identities*, John Wiley and Sons, New York 1968.

Rota, G.-C.
[1] *On the foundations of combinatorial theory I: Theory of Möbius functions*, Z. Wahrscheinlichkeitstheorie und Verw. Gebiete 2 (1964), str. 340–368.
[2] *The number of partitions of a set*, Amer. Math. Monthly 71 (1964), str. 498–504.

Rota, G.-C., Kahaner, D., Odlyzko, A.
[1] *On the foundations of combinatorial theory VIII: Finite operator calculus*, J. Math. Anal. Appl. 42 (1973), str. 684–760.

Room, T. G.
[1] *A new type of magic square*, Math. Gaz. 39 (1955), str. 307.

Ryser, H. J.

[1] *A combinatorial theorem with an application to Latin rectangles*, Proc. Amer. Math. Soc. 2 (1951), str. 550–552.

[2] *Combinatorial mathematics*, Carus Math. Monographs nr 14, Math. Assoc. of America, New York 1963.

[3] *An extension of a theorem of de Bruijn and Erdős on combinatorial designs*, J. Algebra 10 (1968), str. 246–261.

[4] *Symmetric designs and related configurations*, J. Combin. Theory 12 (1972), str. 98–111.

[5] *Variants of cyclic difference sets*, Proc. Amer. Math. Soc. 41 (1973), str. 45–50.

Sanders, J.

[1] *A generalization of a theorem of Schur*, Doctoral Dissertation, Yale University, New Haven, CT 1968.

Schmidt, W. M.

[1] *Two combinatorial theorems on arithmetic progressions*, Duke Math. J. 29 (1962), str. 129–140.

[2] *Ein kombinatorisches Problem von P. Erdős und A. Hajnal*, Acta Math. Acad. Sci. Hung. 15 (1964), str. 373–374.

Schur, I.

[1] *Über die Kongruenz* $x^m + y^m = z^m \pmod{p}$, Jahresber. Deutsch. Math.-Verein. 25 (1916), str. 114–117.

Schützenberger, M. P.

[1] *Contribution aux applications statistiques de la théorie de l'information*, Publ. Inst. Stat. Univ. Paris 3 (1954), str. 5–117.

Shrikhande, S. S.

[1] *The impossibility of certain symmetrical balanced incomplete block design*, Ann. Math. Stat. 21 (1950), str. 106–111.

Sierpiński, W.

[1] *Arytmetyka teoretyczna*, wyd. 3, PWN, Warszawa 1966.

Singer, J.

[1] *A theorem in finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. 43 (1938), str. 377–385.

Singhi, N. M., Shirikhande, S. S.

[1] *On the λ-design conjecture*, Utilitas Math. 9 (1976), str. 301–318.

Slepian, D.

[1] *Two theorems on a particular crossbar switching network*, Nie opublikowany artykuł, 1952.

Sloane, N. J. A.

[1] *Error-correcting codes and invariant theory: New applications of a nineteenth-century technique*, Amer. Math. Monthly 84 (1977), str. 82–107.

Smorynski, C.

[1] *Some rapidly growing functions*, Math. Intelligencer 2 (1980), str. 149–154.

Spencer, J.

[1] *Restricted Ramsey configurations*, J. Combin. Theory 19 (1975), str. 278–286.

[2] *Ramsey's theorem – a new lower bound*, J. Combin. Theory 18 (1975), str. 108–115.

Sperner, E.

[1] *Ein Satz über Untermengen einer endlichen Menge*, Math. Z. 27 (1928), str. 544–548.

Stanley, R. P.

[1] *Generating functions*, w: *Studies in combinatorics*, MAA Studies in Math., vol. 17 (1978), str. 100–141.

Stanton, R. G., Mullin, R. C.
[1] *Construction of Room squares*, Ann. Math. Statist. 39 (1968), str. 1540–1548.

Steiner, J.
[1] *Combinatorische Aufgabe*, J. Reine Angew. Math. 45 (1853), str. 181–182.

Surányi, J.
[1] *Megjegyzések a kinai matematika történetének egy problémájárol*, Mat. Lapok 6 (1955), str. 30–35.

Szemerédi, E.
[1] *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. 2⁻ (1975), str. 199–243.

Szpilrajn, E.
[1] *Sur l'extension de l'ordre partiel*, Fund. Math. 6 (1930), str. 386–389.

Tarry, G.
[1] *Le problème de 36 officieurs*, Compte Rendu de l'Association Française pour l'Avancement de Science Naturel 1 (1900), str. 122–123; 2 (1901), str. 170–203.

Tarski, A.
[1] *A lattice-theoretic fixpoint theorem and its applications*, Pacific J. Math. 5 (1955), str. 285–309.

Taylor, A. D.
[1] *A note on van der Waerden's theorem*, J. Combin. Theory, Ser. A 33 (1982), str. 215–219.

Touchard, J.
[1] *Sur un problème de permutations*, C. R. Acad. Sci. Paris 198 (1934), str. 631–633.

Turán, P.
[1] *Egy gráfelméleti szélsőérték feladotról*, Mat. Fiz. Lapok 48 (1941), str. 436–452, P. też: *On the theory of graphs*, Colloq. Math. 3 (1954), str. 19–30.

Tverberg, H.
[1] *On Dilworth's decomposition theorem for partially ordered sets*, J. Combin. Theory 3 (1967), str. 305–306.

van der Waerden, B. I.
[1] *Beweis einer Baudetschen Vermutung*, Nieuw. Arch. Wisk. 15 (1927), str. 212–216.

Wallis, W. P.
[1] *Solution of the Room square existence problem*, J. Combin. Theory 17 (1974), str. 379–383.

Wallis, W. D., Street, A. P., Wallis, J. S.
[1] *Combinatorics: Room squares, sum-free sets, Hadamard matrices*, Springer-Verlag, Berlin 1972.

Weisner, L.
[1] *Abstract theory of inversion of finite series*, Trans. Amer. Math. Soc. 38 (1935), str. 474–484.

Wilenkin, N. J.
[1] *Kombinatoryka*, PWN, Warszawa 1972.

Williamson, J.
[1] *Hadamard's determinant theorem and the sum of few squares*, Duke J. Math. 11 (1944), str. 65–81.

Wilson, R. M.
[1] *An existence theory for pairwise balanced designs I, Composition theorems and morphisms*, J. Combin. Theory 13 (1972), str. 220–245.
[2] *An existence theory for pairwise balanced designs II, The structure of PBD-closed sets and the existence conjectures*, J. Combin. Theory 13 (1972), str. 246–273.
[3] *An existence theory for pairwise balanced designs III, Proof of the existence conjectures*, J. Combin. Theory Ser. A 18 (1975), str. 71–79.

de Witte, P.

[1] *Some new properties of semi-tactical λ-spaces*, Bull. Soc. Math. Belg. 19 (1967), str. 13–24.

Woodall, D. R.

[1] *Square λ-linked designs*, Proc. London Math. Soc. (3) 20 (1970), str. 669–687.

Yackel, J.

[1] *Inequalities and asymptotic bounds for Ramsey numbers*, J. Combin. Theory 13 (1972), str. 56–68.

Yamamoto, K.

[1] *Logarithmic order of free distinctive lattices*, J. Math. Soc. Japan 6 (1954), str. 343–353.

SKOROWIDZ

(opracował Julian Panz)

SPIS RZECZY

PAŃSTWOWE
WYDAWNICTWO NAUKOWE

Wydanie I. Nakład 4820+180. Ark. wyd. 29,5. Ark. druk. 29. Papier offsetowy kl. V 70 g, 70 × 100 cm. Oddano do składania w czerwcu 1983 r. Podpisano do druku w kwietniu 1986 r. Druk ukończono w maju 1986 r. Zam. nr 2246/83
Z-7. Cena zł 360,–

WROCŁAWSKA DRUKARNIA NAUKOWA